UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590 01/06/2009

Williams M Lee Jr.
2351 Boulevard Alfred-Nobel
St Laurent, QC H4S 2A9
CANADA

EXAMINER	
AHMED, SALMAN	
ART UNIT	PAPER NUMBER
2419	

DATE MAILED: 01/06/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,162	09/30/2003	Julian Mitchell	16075IDUS01U	5559

TITLE OF INVENTION: CONVERTOR SHARED BY MULTIPLE VIRTUAL PRIVATE NETWORKS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	04/06/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,162	09/30/2003	Julian Mitchell	16075IDUS01U	5559

7590 01/06/2009

EXAMINER	
AHMED, SALMAN	
ART UNIT	PAPER NUMBER
2419	

DATE MAILED: 01/06/2009

Williams M Lee Jr.
2351 Boulevard Alfred-Nobel
St Laurent, QC H4S 2A9
CANADA

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 983 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 983 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

7590 01/06/2009

Williams M Lee Jr.
2351 Boulevard Alfred-Nobel
St Laurent, QC H4S 2A9
CANADA

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,162	09/30/2003	Julian Mitchell	16075IDUS01U	5559

TITLE OF INVENTION: CONVERTOR SHARED BY MULTIPLE VIRTUAL PRIVATE NETWORKS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	04/06/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
AHMED, SALMAN	2419	370-395530

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Notice of Allowability	Application No.	Applicant(s)	
	10/675,162	MITCHELL ET AL.	
	Examiner	Art Unit	
	SALMAN AHMED	2419	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendments filed on 9/15/2008*.

2. ☒ The allowed claim(s) is/are *30, 32-34, 36-47, 49-51, 53-64 and 66-74 (Currently remumbeered to 1-40 respectively)*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Salman Ahmed
Examiner
Art Unit: 2419

Allowable Subject Matter

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

Claim 30 line 10 "signalling" has been changed to –signaling--.

Claim 55 line 2 "signalling" has been changed to –signaling--.

Claim 47 line 12 "signalling" has been changed to –signaling--.

Claim 64 line 8 "signalling" has been changed to –signaling--.

Claim 69 line 3 "signalling" has been changed to –signaling--.

Claim 74 line 12 "signalling" has been changed to –signaling--.

Allowable Subject Matter

1. Claims 30, 32-34, 36-47, 49-51, 53-64 and 66-74 are allowed.

Reason for Allowance

2. The following is an examiner's statement of reasons for allowance:

The prior art of record does not teach the following:

In regards to claim 30 the prior art does not teach a second data network connected to the plurality of VPNs via the first data network, the second data network using a network addressing scheme that is different to a network addressing scheme used by at least one of plurality of VPNs; a VPN gateway interfacing the first data

network and a call server in the second data network, the VPN gateway being configured to pass communication session signaling traffic between an entity in one of plurality of VPNs and the call server for establishing a communication session between entity in one of plurality of VPNs and an entity in an external Time Division Multiplex 'TDM' network, external TDM network handling communication session bearer traffic in a TDM format different to a packet data format of the first data network; and a VPN converter interfacing the first and second data networks and directly interfacing the first data network to external TDM network, the VPN converter being configured to receive bearer traffic relating to communication session established between entity in one of plurality of VPNs and the entity in the external TDM network and to convert bearer traffic between the packet data format of the first data network and the TDM format used in the external TDM network.

In regards to claim 47 the prior art does not teach second data network using a network addressing scheme that is different to a network addressing scheme used by at least one of plurality of VPNs; a VPN gateway interfacing the first data network and a call server in the second data network; and a VPN converter interfacing the first and second data networks; the method comprising the steps of: directly interfacing the first data network to an external Time Division Multiplex 'TDM' network; configuring the VPN gateway to pass communication session signaling traffic between an entity in one of plurality of VPNs and the call server for establishing a communication session between entity in one of plurality of VPNs and an entity in external TDM network, external TDM network handling communication session bearer traffic in a TDM format

different to at a packet data format of the first data network; and configuring the VPN converter to receive bearer traffic relating to communication session established between entity in one of plurality of VPNs and the entity in the external TDM network and to convert bearer traffic between a the packet data format of the first data network and the TDM format used in the external TDM network.

In regards to claim 64 the prior art does not teach second data network using a network addressing scheme that is different to a network addressing scheme used by at least one of plurality of VPNs; and a VPN gateway interfacing the first data network and a call server in the second data network, the VPN gateway being configured to pass communication session signaling traffic between an entity in one of plurality of VPNs and the call server for establishing a communication session between entity in one of plurality of VPNs and an entity in an external Time Division Multiplex 'TDM' network, external TDM network handling communication session bearer traffic in a TDM format different to a packet data format of the first data network; the VPN converter comprising: interfaces for interfacing the first and second data networks and directly interfacing the first data network to external TDM network, means for receiving bearer traffic relating to communication session established between entity in one of plurality of VPNs and the entity in the external TDM network; and means for converting bearer traffic between a the packet data format of the first data network and the TDM format used in the external TDM network.

In regards to claim 74 the prior art does not teach the second data network using a network addressing scheme that is different to a network addressing scheme used by at least one of plurality of VPNs; a VPN gateway interfacing the first data network and a call server in the second data network; and a VPN converter interfacing the first and second data networks and directly interfacing the first data network to an external Time Division Multiplex 'TDM' network; the steps of: causing the VPN gateway to pass communication session signaling traffic between an entity in one of plurality of VPNs and the call server for establishing a communication session between entity in one of plurality of VPNs and an entity in external TDM network, external TDM network handling communication session bearer traffic in a TDM format different to a packet data format of the first data network; and causing the VPN converter to receive bearer traffic relating to communication session established between entity in one of plurality of VPNs and the entity in the external TDM network and to convert bearer traffic between the packet data format of the first data network and the TDM format used in the external TDM network.

The prior art alone or in combination fails to jointly suggest or teach the claimed combination of features as taught by the instant application. Therefore claims 30, 32-34, 36-47, 49-51, 53-64 and 66-74 are to be deemed allowable over prior art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SALMAN AHMED whose telephone number is (571)272-8307. The examiner can normally be reached on 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. A./

Examiner, Art Unit 2419

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2419

Notice of References Cited	Application/Control No. 10/675,162	Applicant(s)/Patent Under Reexamination MITCHELL ET AL.	
	Examiner SALMAN AHMED	Art Unit 2419	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2001/0012775 A1	08-2001	Modzelesky et al.	455/427
*	B	US-2003/0147402 A1	08-2003	Brahim, Hamid Ould	370/395.53
*	C	US-2004/0105459 A1	06-2004	Mannam, Raghu	370/465
*	D	US-2004/0136534 A1	07-2004	Stiscia et al.	380/256
*	E	US-2004/0136712 A1	07-2004	Stiscia et al.	398/060
*	F	US-2005/0047713 A1	03-2005	Antosik, Roman	385/024
*	G	US-2005/0068942 A1	03-2005	Chu et al.	370/352
*	H	US-6,879,680 B2	04-2005	Donovan et al.	379/220.01
*	I	US-2005/0105708 A1	05-2005	Kouchri et al.	379/219
*	J	US-2005/0111469 A1	05-2005	Howell, Royal Dean	370/410
*	K	US-2005/0141504 A1	06-2005	Rembert et al.	370/392
*	L	US-2005/0226210 A1	10-2005	Martin, James	370/351
*	M	US-2005/0220148 A1	10-2005	DelRegno et al.	370/498

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	EP1768343A2	03-1007	EPO	Croak et al.	
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	MPLS and next generation access networks; Kankkunen, A.; Universal Multiservice Networks, 2000. ECUMN 2000. 1st European Conference on 2-4 Oct. 2000 Page(s):5 - 16
	V	Hybrid transport solutions for TDM/data networking services; Hernandez-Valencia, E.; Communications Magazine, IEEE□□Volume 40, Issue 5, May 2002 Page(s):104 - 112
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/675,162	Applicant(s)/Patent Under Reexamination MITCHELL ET AL.	
	Examiner SALMAN AHMED	Art Unit 2419	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0220143 A1	10-2005	DelRegno et al.	370/471
*	B	US-2005/0220014 A1	10-2005	DelRegno et al.	370/230
*	C	US-2006/0239242 A1	10-2006	Huffschmid, Norbert	370/352
*	D	US-2007/0064594 A1	03-2007	Norton, T. ReNae	370/218
*	E	US-2007/0140250 A1	06-2007	McAllister et al.	370/392
*	F	US-7,304,986 B2	12-2007	Allen et al.	370/356
*	G	US-7,330,463 B1	02-2008	Bradd et al.	370/352
*	H	US-7,385,995 B2	06-2008	Stiscia et al.	370/412
*	I	US-2008/0285438 A1	11-2008	Marathe et al.	370/220
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 768 343 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.03.2007 Bulletin 2007/13

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **06121167.8**

(22) Date of filing: **25.09.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **26.09.2005 US 234919**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

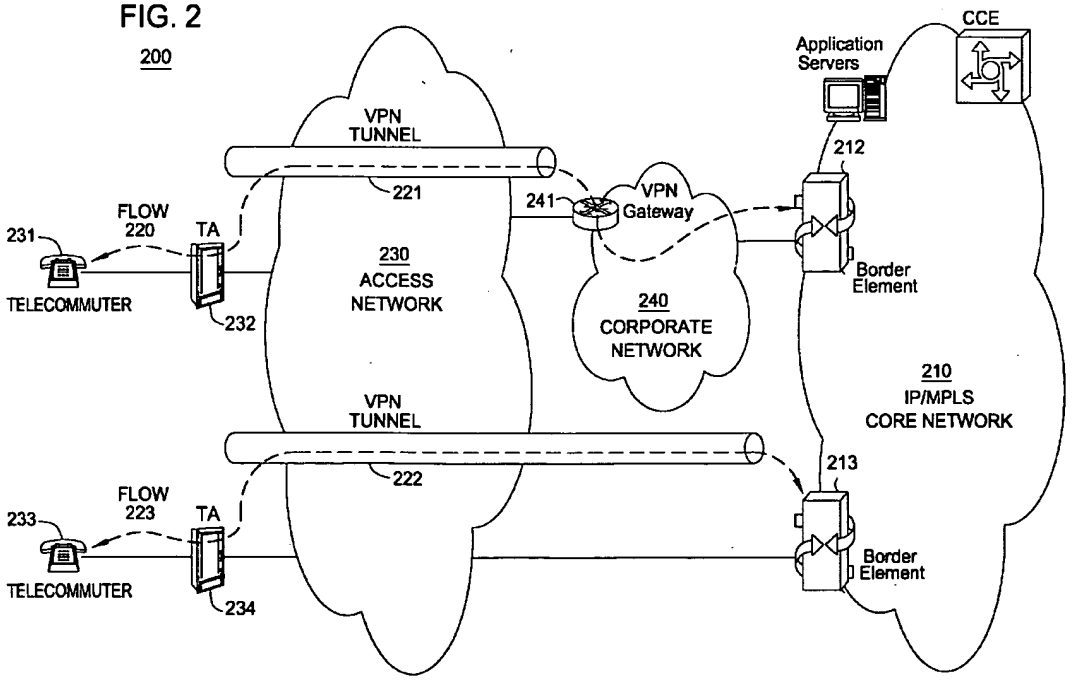
(72) Inventors:
- **Croak, Marian**
  Fair Haven, NJ 07704 (US)
- **Eslambolchi, Hossein**
  Los Altos Hills, CA 94022 (US)

(74) Representative: **Harding, Richard Patrick**
Marks & Clerk,
4220 Nash Court,
Oxford Business Park South
Oxford OX4 2RU (GB)

(54) Method and apparatus for activating alternative virtual private network protocols

(57) A method and apparatus for enabling enterprise customers to detect VPN protocol blocking by access network providers and provides client VPN software with instructions to activate another VPN protocol such as Secure Socket Layer (SSL) that is less likely to be blocked by their provider are disclosed. For instance, if the access network provider blocks the IPSec VPN protocol, the client VPN software will switch to an alternative VPN protocol, such as Secure Socket Layer (SSL) protocol, Layer 2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP), to connect to the VoIP network. The SSL, L2TP, and PPTP protocols are all VPN protocols designed to enable encrypted and authenticated communications across the public Internet.

FIG. 2



EP 1 768 343 A2

Description

[0001] The present invention relates generally to communication networks and, more particularly, to a method and apparatus for activating alternative Virtual Private Network (VPN) protocols in accessing communication networks, e.g., packet networks such as Voice over Internet Protocol (VoIP) networks.

BACKGROUND OF THE INVENTION

[0002] For security reasons, remote workers access their corporate sites and VoIP services through VPN tunnels using IP Security (IPSec) VPN protocols. Broadband access network providers will frequently block the IPSec protocol unless users are subscribed to arrangements that frequently charge the subscribers twice the price of regular residential subscriptions with no added value. IPSec is a security protocol defined by the IETF (Internet Engineering Task Force) that provides authentication and encryption over the public Internet. A VPN protocol is designed to enable encrypted and authenticated communications across the public Internet.

[0003] Therefore, a need exists for a method and apparatus for activating alternative Virtual Private Network (VPN) protocols in accessing a packet network, e.g., a VoIP network.

SUMMARY OF THE INVENTION

[0004] In one embodiment, the present invention enables enterprise customers to detect VPN protocol blocking by access network providers and provides client VPN software with instructions to activate another VPN protocol such as Secure Socket Layer (SSL) that is less likely to be blocked by their provider. For instance, if the access network provider blocks the IPSec VPN protocol, the client VPN software will switch to an alternative VPN protocol, such as Secure Socket Layer (SSL) protocol, Layer 2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP) and the like, to connect to the VoIP network. The SSL, L2TP, and PPTP protocols are all VPN protocols designed to enable encrypted and authenticated communications across the public Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The teaching of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

[0006] FIG. 1 illustrates an exemplary Voice over Internet Protocol (VoIP) network related to the present invention;

[0007] FIG. 2 illustrates an example of using Virtual Private Network (VPN) protocols in a VoIP network related to the present invention;

[0008] FIG. 3 illustrates a flowchart of a method for activating alternative Virtual Private Network (VPN) protocols in a VoIP network of the present invention; and

[0009] FIG. 4 illustrates a high level block diagram of a general purpose computer suitable for use in performing the functions described herein.

[0010] To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

DETAILED DESCRIPTION

[0011] To better understand the present invention, FIG. 1 illustrates a communication architecture 100 having an example network, e.g., a packet network such as a VoIP network related to the present invention. Exemplary packet networks include internet protocol (IP) networks, asynchronous transfer mode (ATM) networks, frame-relay networks, and the like. An IP network is broadly defined as a network that uses Internet Protocol to exchange data packets. Thus, a VoIP network or a SoIP (Service over Internet Protocol) network is considered an IP network.

[0012] In one embodiment, the VoIP network may comprise various types of customer endpoint devices connected via various types of access networks to a carrier (a service provider) VoIP core infrastructure over an Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) based core backbone network. Broadly defined, a VoIP network is a network that is capable of carrying voice signals as packetized data over an IP network. The present invention is described below in the context of an illustrative VoIP network. Thus, the present invention should not be interpreted to be limited by this particular illustrative architecture.

[0013] The customer endpoint devices can be either Time Division Multiplexing (TDM) based or IP based. TDM based customer endpoint devices 122, 123, 134, and 135 typically comprise of TDM phones or Private Branch Exchange (PBX). IP based customer endpoint devices 144 and145 typically comprise IP phones or IP PBX. The Terminal Adaptors (TA) 132 and 133 are used to provide necessary interworking functions between TDM customer endpoint devices, such as analog phones, and packet based access network technologies, such as Digital Subscriber Loop (DSL) or Cable broadband access networks. TDM based customer endpoint devices access VoIP services by using either a Public Switched Telephone Network (PSTN) 120, 121 or a broadband access network via a TA 132 or 133. IP based customer endpoint devices access VoIP services by using a Local Area Network (LAN) 140 and 141 with a VoIP gateway or router 142 and 143, respectively.

[0014] The access networks can be either TDM or packet based. A TDM PSTN 120 or 121 is used to support TDM customer endpoint devices connected via traditional phone lines. A packet based access network, such as Frame Relay, ATM, Ethernet or IP, is used to support IP based customer endpoint devices via a customer LAN,

e.g., 140 with a VoIP gateway and router 142. A packet based access network 130 or 131, such as DSL or Cable, when used together with a TA 132 or 133, is used to support TDM based customer endpoint devices.

[0015] The core VoIP infrastructure comprises of several key VoIP components, such the Border Element (BE) 112 and 113, the Call Control Element (CCE) 111, and VoIP related servers 114. The BE resides at the edge of the VoIP core infrastructure and interfaces with customers endpoints over various types of access networks. A BE is typically implemented as a Media Gateway and performs signaling, media control, security, and call admission control and related functions. The CCE resides within the VoIP infrastructure and is connected to the BEs using the Session Initiation Protocol (SIP) over the underlying IP/MPLS based core backbone network 110. The CCE is typically implemented as a Media Gateway Controller or a softswitch and performs network wide call control related functions as well as interacts with the appropriate VoIP service related servers when necessary. The CCE functions as a SIP back-to-back user agent and is a signaling endpoint for all call legs between all BEs and the CCE. The CCE may need to interact with various VoIP related servers in order to complete a call that require certain service specific features, e.g. translation of an E.164 voice network address into an IP address.

[0016] For calls that originate or terminate in a different carrier, they can be handled through the PSTN 120 and 121 or the Partner IP Carrier 160 interconnections. For originating or terminating TDM calls, they can be handled via existing PSTN interconnections to the other carrier. For originating or terminating VoIP calls, they can be handled via the Partner IP carrier interface 160 to the other carrier.

[0017] In order to illustrate how the different components operate to support a VoIP call, the following call scenario is used to illustrate how a VoIP call is setup between two customer endpoints. A customer using IP device 144 at location A places a call to another customer at location Z using TDM device 135. During the call setup, a setup signaling message is sent from IP device 144, through the LAN 140, the VoIP Gateway/Router 142, and the associated packet based access network, to BE 112. BE 112 will then send a setup signaling message, such as a SIP-INVITE message if SIP is used, to CCE 111. CCE 111 looks at the called party information and queries the necessary VoIP service related server 114 to obtain the information to complete this call. If BE 113 needs to be involved in completing the call; CCE 111 sends another call setup message, such as a SIP-INVITE message if SIP is used, to BE 113. Upon receiving the call setup message, BE 113 forwards the call setup message, via broadband network 131, to TA 133. TA 133 then identifies the appropriate TDM device 135 and rings that device. Once the call is accepted at location Z by the called party, a call acknowledgement signaling message, such as a SIP-ACK message if SIP is used, is sent in the reverse direction back to the CCE 111. After the CCE 111 receives the call acknowledgement message, it will then send a call acknowledgement signaling message, such as a SIP-ACK message if SIP is used, toward the calling party. In addition, the CCE 111 also provides the necessary information of the call to both BE 112 and BE 113 so that the call data exchange can proceed directly between BE 112 and BE 113. The call signaling path 150 and the call media path 151 are illustratively shown in FIG. 1. Note that the call signaling path and the call media path are different because once a call has been setup up between two endpoints, the CCE 111 does not need to be in the data path for actual direct data exchange.

[0018] Media Servers (MS) 115 are special servers that typically handle and terminate media streams, and to provide services such as announcements, bridges, transcoding, and Interactive Voice Response (IVR) messages for VoIP service applications.

[0019] Note that a customer in location A using any endpoint device type with its associated access network type can communicate with another customer in location Z using any endpoint device type with its associated network type as well. For instance, a customer at location A using IP customer endpoint device 144 with packet based access network 140 can call another customer at location Z using TDM endpoint device 123 with PSTN access network 121. The BEs 112 and 113 are responsible for the necessary signaling protocol translation, e.g., SS7 to and from SIP, and media format conversion, such as TDM voice format to and from IP based packet voice format.

[0020] For security reasons, remote workers access their corporate sites and VoIP services through VPN tunnels using IP Security (IPSec) VPN protocols. Broadband access network providers will frequently block the IPSec protocol unless users are subscribed to arrangements that frequently charge the subscribers twice the price of regular residential subscriptions with no added value. When a particular VPN protocol is blocked by an access network provider, subscribers need to be aware of it and then switch to a different VPN protocol that is not blocked by the access network provider. IPSec is a security protocol defined by the IETF (Internet Engineering Task Force) that provides authentication and encryption over the public Internet. A VPN protocol is designed to enable encrypted and authenticated communications across the public Internet.

[0021] To address this criticality, the present invention enables enterprise customers to detect VPN protocol blocking by access network providers and provides client VPN software with instructions to activate another VPN protocol such as Secure Socket Layer (SSL) that is less likely to be blocked by their provider. For instance, if the access network provider blocks the IPSec VPN protocol, the client VPN software will switch to an alternative VPN protocol, such as Secure Socket Layer (SSL) protocol, Layer2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP) and the like, to connect to the VoIP network. The SSL, L2TP, and PPTP protocols are

all VPN protocols designed to enable encrypted and authenticated communications across the public Internet.

[0022] FIG. 2 illustrates an exemplary communication architecture 200 for using Virtual Private Network (VPN) protocols in a packet network, e.g., a VoIP network related to the present invention. In FIG. 2, in one embodiment of the present invention, telecommuter 231 via TA 232 remotely accesses corporate network 240 to perform work related activities, including using VoIP services subscribed by the corporation. Telecommuter 231 uses VPN protocol via VPN tunnel 221 to securely access corporate network 240 through VPN Gateway 241. VPN tunnel 221 provides secured communication between telecommuter 231 and VPN Gateway 241 over the public internet access network 230 (e.g., an Internet Protocol (IP) network). In FIG. 2, telecommuter 231 uses the VoIP services subscribed by the corporation via signaling flow 220. In on embodiment, BE 212 can actively detects and determines the VPN protocols blocked by access network 230. Common VPN protocol used are, but not limited to, IPSec, SSL, PPTP, and L2TP protocols. If BE 212 has determined that access network 230 is blocking the IPSec protocol, BE 212 will signal the VPN client software used by telecommuter 231 to use an alternative protocol, such as SSL, that is not blocked by access network 230. Using the SSL protocol, telecommuter can then connect to corporate network 240, using the uninterrupted signaling 220, to access the subscribed VoIP services. If SSL is also blocked, BE 212 can attempt to use other available VPN protocols, such as L2TP or PPTP, to communicate with telecommuter 231.

[0023] In FIG. 2, in another embodiment of the present invention, telecommuter 233 via TA 234 uses VPN protocol via VPN tunnel 222 over access network 230 to securely access VoIP services subscribed by the corporation that telecommuter 233 works for. VPN tunnel 222 provides secured communication between telecommuter 233 and VoIP network 210 over the public internet access network 230. In FIG. 2, telecommuter 233 uses the VoIP services subscribed by the corporation via signaling flow 223. BE 213 can actively detects and determines the VPN protocols blocked by access network 230. Common VPN protocol used are, but not limited to, IPSec, SSL, PPTP, and L2TP protocols. If BE 213 has determined that access network 230 is blocking the IPSec protocol, BE 213 will signal the VPN client software used by telecommuter 233 to use an alternative protocol, such as SSL, that is not blocked by access network 230. Using the SSL protocol, telecommuter can then connect to the VoIP network, using the uninterrupted signaling 223, to access the subscribed VoIP services. If SSL is also blocked, BE 213 can attempt to use other available VPN protocols, such as L2TP or PPTP, to communicate with telecommuter 233.

[0024] FIG. 3 illustrates a flowchart of a method 300 for activating alternative Virtual Private Network (VPN) protocols in a packet network, e.g., VoIP network of the present invention. Method 300 starts in step 305 and proceeds to step 310.

[0025] In step 310, the method attempts to initiate a VPN tunnel test using a selected VPN protocol to signal to an endpoint device by a BE. For example, the testing may start when an endpoint device signals that it wants to establish secured communication.

[0026] In step 320, the method checks if the selected VPN protocol is blocked by the access network. If the selected VPN protocol is blocked by the access network, the method proceeds to step 330; otherwise, the method proceeds to step 350. Available VPN protocols that can be selected include, but are not limited to, IPSec, SSL, L2TP, and PPTP protocols.

[0027] In step 330, the method checks if all available VPN protocols have been tested against the access network. If all available VPN protocols have been exhausted, the method proceeds to step 370; otherwise, the method proceeds to step 340.

[0028] In step 340, the method selects the next available VPN protocol and proceeds back to step 310.

[0029] In step 350, the method signals to the VoIP endpoint device to use the selected VPN protocol to establish a VPN tunnel. Namely, a VPN protocol has been detected that is not being blocked.

[0030] In step 360, the method activates a VPN tunnel between VoIP endpoint device and the corporate network.

[0031] In step 370, the method alerts the customer that all available VPN protocols are blocked by the access network. The method ends in step 380.

[0032] FIG. 4 depicts a high level block diagram of a general purpose computer suitable for use in performing the functions described herein. As depicted in FIG. 4, the system 400 comprises a processor element 402 (e.g., a CPU), a memory 404, e.g., random access memory (RAM) and/or read only memory (ROM), a module 405 for activating alternative VPN protocols, and various input/output devices 406 (e.g., storage devices, including but not limited to, a tape drive, a floppy drive, a hard disk drive or a compact disk drive, a receiver, a transmitter, a speaker, a display, a speech synthesizer, an output port, and a user input device (such as a keyboard, a keypad, a mouse, and the like)).

[0033] It should be noted that the present invention can be implemented in software and/or in a combination of software and hardware, e.g., using application specific integrated circuits (ASIC), a general purpose computer or any other hardware equivalents. In one embodiment, the present module or process 405 for activating alternative VPN protocols can be loaded into memory 404 and executed by processor 402 to implement the functions as discussed above. As such, the present process 405 for activating alternative VPN protocols (including associated data structures) of the present invention can be stored on a computer readable medium or carrier, e.g., RAM memory, magnetic or optical drive or diskette and the like.

[0034] While various embodiments have been de-

scribed above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

Claims

1. A method for selecting a Virtual Private Network, VPN, protocol in accessing a communication network, comprising:

   testing a first VPN protocol from a plurality of available VPN protocols to signal to an endpoint device by an edge component of said communication network over an access network; and selecting an alternative VPN protocol from said plurality of available VPN protocols to signal to said endpoint device by said edge component of said communication network over said access network if said first VPN protocol is blocked by said access network.

2. The method of claim 1, wherein said communication network is a Voice over Internet Protocol, VoIP, network or a Service over Internet Protocol, SoIP network.

3. The method of claim 1 or 2, wherein said access network is an Internet Protocol, IP, network.

4. The method of claim 1, 2 or 3, wherein said edge component is a Border Element, BE.

5. The method of any one of the preceding claims, wherein said plurality of available VPN protocols comprise at least two of: an IP Security, IPSec, protocol, a Secure Socket Layer, SSL, protocol, a Layer 2 Tunneling Protocol, L2TP, or a Point-to-Point Tunneling Protocol, PPTP, protocol.

6. The method of any one of the preceding claims, further comprising:

   using said alternative VPN protocol to establish a VPN tunnel over said access network to said endpoint device if said alternative VPN protocol is not blocked by said access network.

7. The method of any one of the preceding claims, further comprising:

   sending a notification to a network administrator of said endpoint device if all of said plurality of VPN protocols are blocked by said access network.

8. A computer-readable medium having stored thereon a plurality of instructions, the plurality of instructions including instructions which, when executed by a processor, cause the processor to perform the steps of a method for selecting a Virtual Private Network, VPN, protocol in accessing a communication network, comprising:

   testing a first VPN protocol from a plurality of available VPN protocols to signal to an endpoint device by an edge component of said communication network over an access network; and selecting an alternative VPN protocol from said plurality of available VPN protocols to signal to said endpoint device by said edge component of said communication network over said access network if said first VPN protocol is blocked by said access network.

9. The computer-readable medium of claim 8, wherein said communication network is a Voice over Internet Protocol, VoIP, network or a Service over Internet Protocol, SoIP, network.

10. The computer-readable medium of claim 8 or 9, wherein said access network is an Internet Protocol, IP, network.

11. The computer-readable medium of claim 8, 9 or 10, wherein said edge component is a Border Element, BE.

12. The computer-readable medium of any one of claims 8 to 11, wherein said plurality of available VPN protocols comprise at least two of: an IP Security, IPSec, protocol, a Secure Socket Layer, SSL, protocol, a Layer 2 Tunneling Protocol, L2TP, or a Point-to-Point Tunneling Protocol, PPTP, protocol.

13. The computer-readable medium of any one of claims 8 to 12, further comprising:

   using said alternative VPN protocol to establish a VPN tunnel over said access network to said endpoint device if said alternative VPN protocol is not blocked by said access network.

14. The computer-readable medium of any one of claims 8 to 13, further comprising:

   sending a notification to a network administrator of said endpoint device if all of said plurality of VPN protocols are blocked by said access network.

15. An apparatus for selecting a Virtual Private Network,

VPN, protocol in accessing a communication network, comprising:

means for testing a first VPN protocol from a plurality of available VPN protocols to signal to an endpoint device by an edge component of said communication network over an access network; and

means for selecting an alternative VPN protocol from said plurality of available VPN protocols to signal to said endpoint device by said edge component of said communication network over said access network if said first VPN protocol is blocked by said access network.

16. The apparatus of claim 15, wherein said communication network is a Voice over Internet Protocol, VoIP, network or a Service over Internet Protocol, SoIP, network.

17. The apparatus of claim 15 or 16, wherein said access network is an Internet Protocol, IP, network.

18. The apparatus of claim 15, 16 or 17, wherein said edge component is a Border Element, BE.

19. The apparatus of any one of claims 15 to 18, wherein said plurality of available VPN protocols comprise at least two of: an IP Security, IPSec, protocol, a Secure Socket Layer, SSL, protocol, a Layer 2 Tunneling Protocol, L2TP, or a Point-to-Point Tunneling Protocol, PPTP, protocol.

20. The apparatus of any one of claims 15 to 19, further comprising:

means for using said alternative VPN protocol to establish a VPN tunnel over said access network to said endpoint device if said alternative VPN protocol is not blocked by said access network.

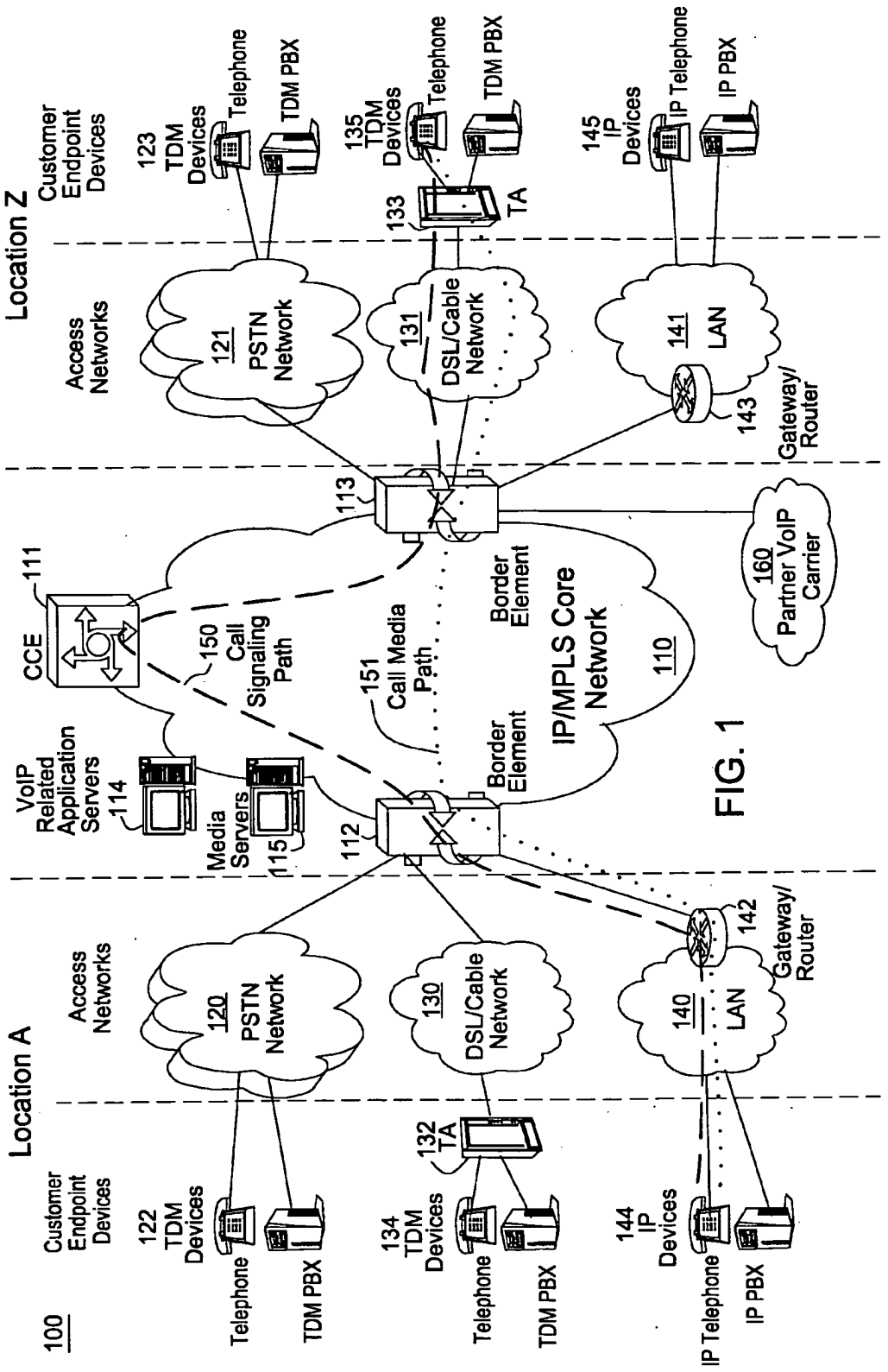

Location Z
Customer Endpoint Devices
123 TDM Devices
Telephone
TDM PBX
135 TDM Devices
Telephone
TDM PBX
133 TA
145 IP Devices
IP Telephone
IP PBX
Access Networks
121 PSTN Network
131 DSL/Cable Network
141 LAN
143 Gateway/ Router
113
CCE
111
150 Call Signaling Path
151 Call Media Path
Border Element
IP/MPLS Core Network
110
160 Partner VoIP Carrier
VoIP Related Application Servers
114
Media Servers
115
112
Border Element
Location A
Access Networks
120 PSTN Network
130 DSL/Cable Network
140 LAN
142 Gateway/ Router
100
Customer Endpoint Devices
122 TDM Devices
Telephone
TDM PBX
132 TA
134 TDM Devices
Telephone
TDM PBX
144 IP Devices
IP Telephone
IP PBX

FIG. 1

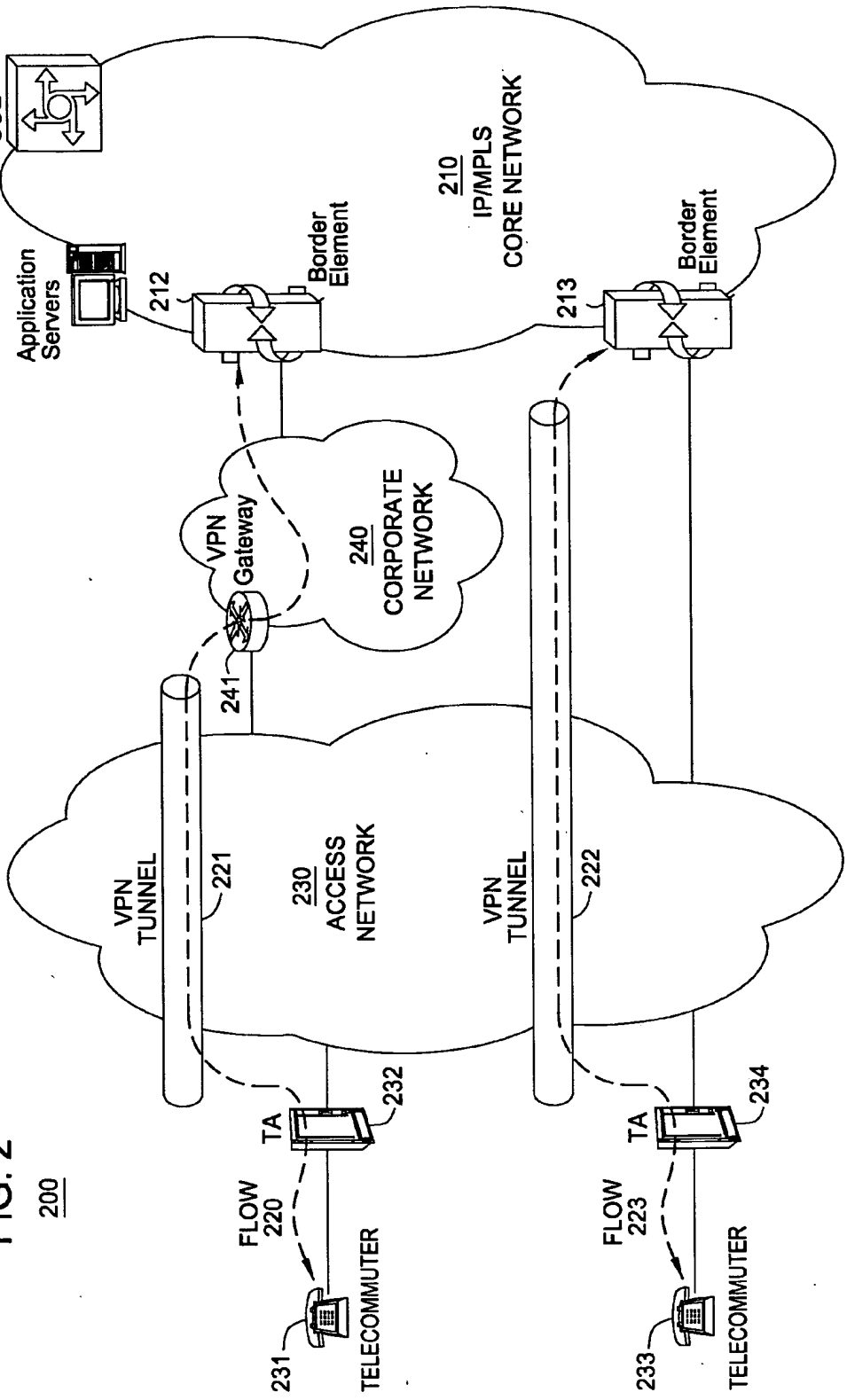

CCE
210
IP/MPLS
CORE NETWORK
Application
Servers
212
Border
Element
213
Border
Element
VPN
Gateway
240
CORPORATE
NETWORK
241
VPN
TUNNEL
221
230
ACCESS
NETWORK
VPN
TUNNEL
222
TA
232
TA
234
FLOW
220
FLOW
223
231
TELECOMMUTER
233
TELECOMMUTER

FIG. 2

200

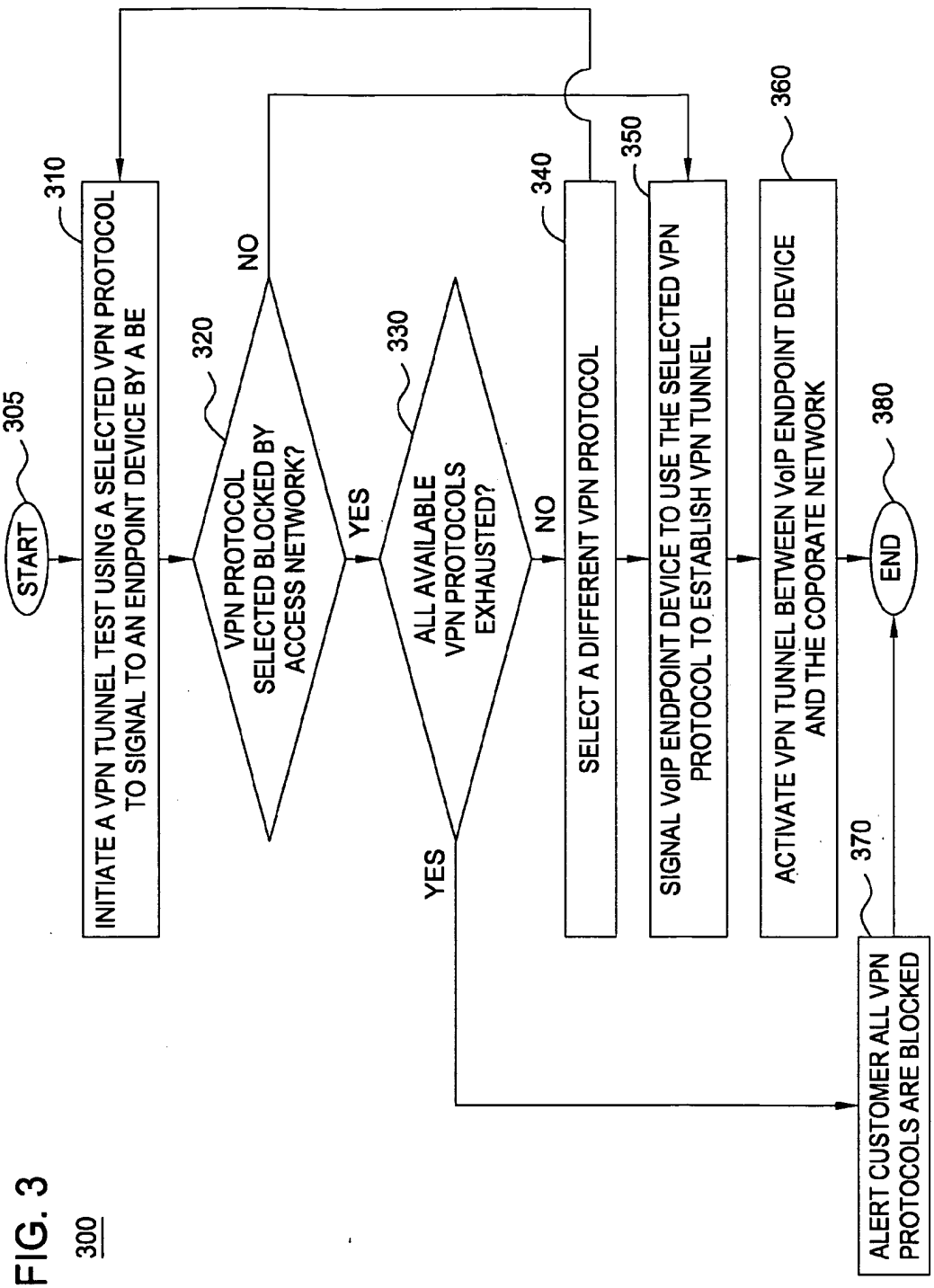

START
305
INITIATE A VPN TUNNEL TEST USING A SELECTED VPN PROTOCOL TO SIGNAL TO AN ENDPOINT DEVICE BY A BE
310
VPN PROTOCOL SELECTED BLOCKED BY ACCESS NETWORK?
320
NO
YES
ALL AVAILABLE VPN PROTOCOLS EXHAUSTED?
330
NO
YES
SELECT A DIFFERENT VPN PROTOCOL
340
SIGNAL VoIP ENDPOINT DEVICE TO USE THE SELECTED VPN PROTOCOL TO ESTABLISH VPN TUNNEL
350
ACTIVATE VPN TUNNEL BETWEEN VoIP ENDPOINT DEVICE AND THE COPORATE NETWORK
360
END
380
ALERT CUSTOMER ALL VPN PROTOCOLS ARE BLOCKED
370

FIG. 3

300

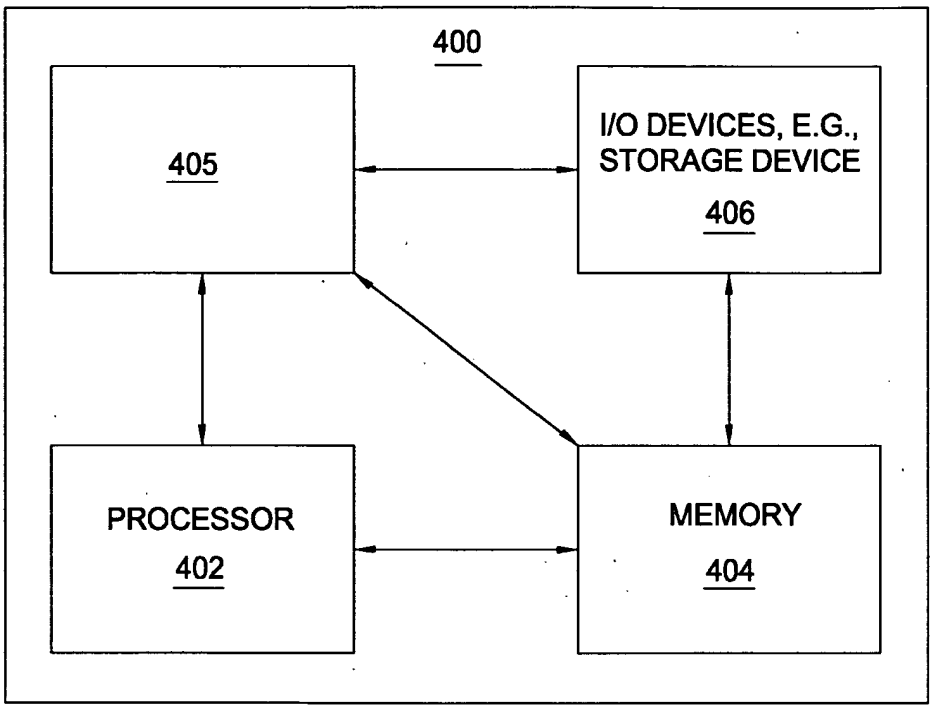

400
405
I/O DEVICES, E.G., STORAGE DEVICE
406
PROCESSOR
402
MEMORY
404

FIG. 4

MPLS and Next Generation Access Networks

Antti KANKKUNEN

Integral Access, Inc.
6 Omni Way
Chelmsford, MA 01824, USA
Tel : +1 978 256 8833 Fax : +1 978 256 8077

Email anttik@integralaccess.com

Abstract : New IP-based technologies for supporting integrated voice and broadband data services over a single link are providing competitive carriers the opportunity to aggressively attack new markets. However, to deliver a comprehensive and competitively priced set of services, carriers must be able to manage QoS. MPLS provides the best alternative for managing QoS and Class of Service (CoS) for IP-based services. This presentation will discuss how carriers can use MPLS to prioritize traffic and provision network bandwidth in order to offer integrated voice/data services, differentiated services and service level agreements.

Keywords : MPLS, QoS, SLA, Integrated Access

1. Abbreviations and acronyms

ADPCM	Adaptive Differential Pulse Code Modulation
AF	Assured Forwarding
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BE	Best Effort
CO	Central Office
CR-LDP	Constraint Based Routing Label Distribution Protocol
DiffServ	Differentiated Services
DLC	Digital Loop Carrier
DS1	Digital Signal 1 (T1 format)
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line (Asymmetric or symmetric)
DWDM	Dense Wavelength Division Multiplexing
E1	G.703 2048kbit/s signal possibly with G.704 framing
EF	Expedited Forwarding
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FR	Frame Relay
G	Guaranteed
GSR	Gigabit Switch Router
HFC	Hybrid Fiber Coax
IAD	Integrated Access Device
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IntServ	Integrated Services
IP	Internet Protocol
IPDC	Internet Protocol Device Control
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN-IC	Local Area Network Inter-Connection
LD	Long Distance
LER	Label Edge Router
LSP	Label Switched Path
MGCP	Media Gateway Control Protocol
MOS	Mean Opinion Score
MPLS	Multi Protocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NMS	Network Management System
OSPF	Open Shortest Path First
PCM	Pulse Code Modulation
PHB	Per Hop Behavior
PON	Passive Optical Network
PoP	Point of Presence
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
ROBO	Regional Office Branch Office
RSVP-TE	Resource Reservation Protocol with Tunneling Extensions
RT	Real Time
RTP	Real time transport protocol
SDH	Synchronous Digital Hierarchy
SG	Signaling Gateway
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SOHO	Small Office Home Office
SONET	Synchronous Optical Network
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TG	Trunk Gateway
TOS	Type of Service

0-7803-6419-8/00/$10.00©2000 IEEE

TSR	Terabit Switch Router
UDP	User Datagram Protocol
VF	Voice Frequency
VoIP	Voice over IP
VoMPLS	Voice over MPLS

2. Vision on network evolution

This section discusses the expected evolution of the public network architecture. The scope of this paper is the network evolution over the next five years.

We believe that all services (voice, video, data, multi-media) are converging towards a single IP-based infrastructure. The network can be divided to two components: The Core Network and the Access Network. This presentation concentrates in the implementation details of the Access Network part. Note that this division should be seen as logical. Some physical network element at the edge of the core may be part of both access network and core network.

2.1. Core Network

We predict that by end of year 2004 more than 95% of the traffic volume (number of bits) transported in the public networks will be generated by applications that are running on top of the IP protocol. Already today the majority of new applications are being developed assuming IP based transport and the desktop is totally ruled by IP. The fact that IP will vastly dominate the traffic volumes implies that the most cost efficient network architecture is one that is optimized for IP. Therefore we expect that the Core Network will migrate towards a two layer protocol stack (Figure 1) containing an optical layer and an IP/MPLS layer. The timeline at the top of Figure 1 indicates the timeframe when the respective protocol stack is predicted to represent the majority of new public multi-service network deployments.

The two layer, IP over glass, protocol stack is in use today for producing best effort type Internet services. A true multi-service network requires advanced QoS, traffic engineering and traffic protection capabilities that are not present in most legacy IP routers.

Today QoS and traffic engineering are provided by an ATM layer and traffic protection is provided by an SDH/SONET layer (see the leftmost stack in Figure 1). Additionally ATM provides a convergence layer for TDM and Frame Relay traffic.

The optimization of the network means that the IP and optical layers will need to absorb these functions as the need for QoS, traffic engineering, protection and multi-service transport will not disappear.

The DiffServ working group of the IETF is chartered to equip the IP layer with QoS capabilities and the MPLS working group is to some extent addressing the first three required functions: QoS, traffic engineering and protection. The first result of the MPLS work is the addition of traffic engineering capabilities to the IP protocol family. This work is essentially complete at this time. QoS work being done in the MPLS working group is based on defining how to integrate DiffServ and MPLS. A less popular alternative, at least in the core network, is the use of MPLS signaling protocol definitions to implicitly define an LSP level QoS model. The RSVP-TE QoS model is based on IntServ (see section 3.2.) and the CR-LDP QoS model is based on traffic parameters that are part of the CR-LDP protocol itself.

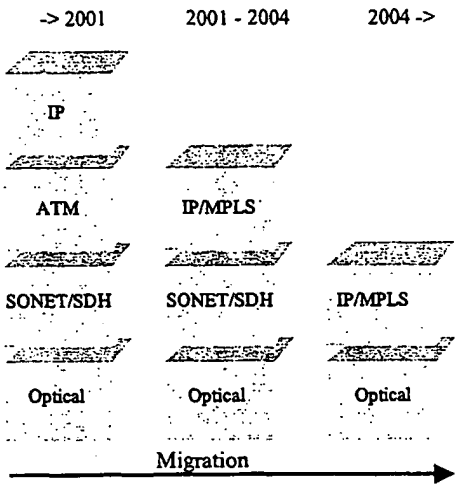
The requirement for multi-service transport, more specifically the requirement for transport of TDM and FR traffic can be solved by the MPLS layer. It is relatively straightforward to define FR to MPLS conversion and it is definitely possible to define circuit emulation over MPLS for TDM traffic. Migrating TDM and FR to an MPLS core does not make sense yet today, as these are both very large services. However over time these services will be replaced by IP based offerings. As soon as TDM and FR represent only a small percentage of the overall service offering, it is attractive to implement tools for integrating the transport of these in one multi-service IP/MPLS network.

As soon as QoS, traffic engineering and multi-service transport are supported by the IP/MPLS layer, network operators can eliminate the ATM layer, as it is no longer needed (see the middle protocol stack of Figure 1). Note that eliminating ATM layer only means getting rid of the ATM control plane. The physical ATM devices and cell based transport can be integrated into the IP/MPLS network by implementing an MPLS control plane in the existing ATM switches.

SONET/SDH will remain an underlying layer due to the fact that the inclusion of protection capabilities in the IP/MPLS layer is a difficult task. These legacy TDM networking technologies can execute protection switching in time scales that are measured in tens of milliseconds. Despite the opposite claims of marketing departments of some IP/MPLS equipment suppliers, this is not reality today with the IP/MPLS layer protection mechanisms.

The solution to the protection problem will be twofold. First it should be recognized that most data applications do not require rerouting to take place in tens of milliseconds. This will allow mechanisms that are based on network layer signaling to be used for protection of data traffic. It can be expected that these types of mechanisms can get down to a couple of seconds of downtime in realistic networking failure scenarios. While a couple of seconds is sufficient for most data applications, it is not acceptable for voice or other demanding applications. Therefore, specific protection mechanisms will be needed that are based on transmitting traffic over two diverse paths. These

types of protection mechanisms need to be developed over the next couple of years to allow the migration to the pure IP over glass protocol stack, which is the rightmost stack in Figure 1.



Legend	
ATM	Asynchronous Transfer Mode
IP	Internet Protocol
MPLS	Multi Protocol Label Switching
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network

Figure 1: Core Network Protocol Stack

We expect that the QoS support in the core network IP/MPLS elements will be based on DiffServ mechanisms. This means that the QoS support is limited to supporting traffic treatment on a packet by packet basis. The traffic management algorithms in the core elements will not recognize application flows or customer connections. The rationale behind this prediction is the fact that this type of QoS is the most economical (and feasible) to implement at high speeds and is sufficient to carry any service. As soon as the core network is running over OC-48c/STM-16 (2.4Gbit/s) links, very strict end-to-end QoS can be provided through a combination of the right access solution and this type of DiffServ core elements. The details of implementing this will be discussed in more detail later in this document.

The core network elements will not be responsible for the DiffServ edge functions like traffic metering, shaping, policing and marking. Instead the Access Network needs to carry out these functions.

It should be noted that part of the protection and traffic engineering functionality will also be implemented in the optical layer. There is currently work in progress to define MPLS based protocols for setting up wavelength paths through an optical switching layer. It is important to keep in mind that the wavelengths are typically used for bandwidths in the order of 2.4Gbit/s and higher. This means that while traffic engineering and protection is useful in the optical layer, the granularity of these functions at the optical layer is much too coarse to eliminate the need for these same functions in the IP/MPLS layer.

The fact that the optical core is going towards an MPLS based control plane is further strengthening the role of MPLS in the future public network architecture.

2.2. Access Network

Large business customers will be served over fiber based access lines and the protocol stack migration will be the same as in the core network (Figure 1). Within the next five years the use of fiber will not be commercially viable in most cases for serving small enterprises (small enterprise = less than 100 employees) and for the low end of the medium sized enterprises (medium size enterprise = less than 500 employees). These customers will be served over copper-based access lines. The practical physical layers are DS1/E1 and DSL.

The practical physical layers for serving residential customers are HFC and DSL.

The discounting of fiber in the previous paragraphs does not mean to imply that we would not see deployment of PON and other fiber architectures that are targeted at the SME and residential markets. Our view is simply that fiber based deployments will represent a small percentage (less than 10%) of the overall access market.

Wireless voice access will be very strong in all market segments but wireless broadband data will not achieve significant deployment during the next five years. This document concentrates on fixed line access and wireless access is not considered further.

In the previous section we predicted that the core of the new public network will consist of two layers: An IP/MPLS layer and an optical layer. We also predicted that the control plane for the optical layer will be based on MPLS protocols.

If the control plane for both layers of the core network is IP/MPLS, what is the optimal control plane for the access part of the network? In our opinion there is only one possible answer to this question. It is naturally an IP/MPLS based control plane as well.

One homogenous control plane end to end is the most optimal way of managing a network. Using the same set of tools throughout the network minimizes the headaches of interoperating different pieces of equipment.

Today's access network is mainly based on TDM. However most people agree that the rigid structure of

TDM is not optimal for serving the future IP based applications.

The only real competitor for an IP/MPLS based access network is an ATM based alternative. The main disadvantage of ATM is the lack of integration with the IP control plane. A service provider ends up having two totally separate control planes which complicates the network. ATM is also a very inefficient transport mechanisms for IP which leads to about 10% bandwidth waste when compared to MPLS. Moreover, ATM has a totally different QoS model than IP leading into non-optimal mapping of QoS end to end over the IP based core. ATM based access is not considered any further in this paper.

While core networks can rely on simple aggregated DiffServ based QoS, access networks cannot depend on statistical phenomena to the same extent. The reason behind this is the fact that the resources in the access network are shared by a smaller number of users. Thus, a situation is probable where all users are simultaneously peaking their resource requirements. As the link speeds in the access network are relatively low it is also more likely that the traffic from a single customer or from a single application will make a significant contribution to the congestion of an individual link. If the service provider wishes to isolate customers from each other and provide fair access to the network resources under congestion, stronger QoS mechanisms than simple packet priority are needed.

Carriers make their money by selling services to end customers. The service is the unit that is the basis for billing and other interfacing towards the customer. Therefore it is a very natural desire for carriers to demand traffic management, which uses a granular per service approach. In an MPLS based access network this can be supported by mapping the traffic of different services into individual LSPs and executing traffic management at LSP level. This way each service can be managed individually and the access network provides optimal isolation between services and shares congested resources between services in a fair manner.

LSP level traffic management means executing per LSP traffic metering, policing, shaping and marking. Real connection admission control is necessary to reject LSPs that would lead into exceeding the available resources. If the service provides wishes to give hard QoS guarantees to any bursty traffic, the access network needs to implement per LSP queuing for such traffic classes.

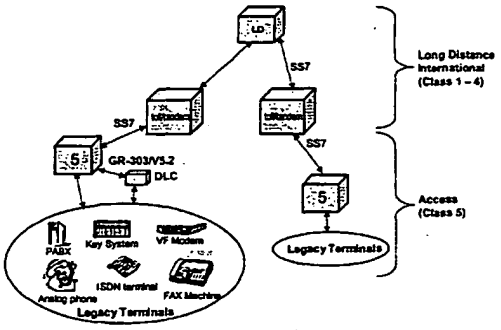
We do not feel that per application flow traffic management would be practical inside the public network infrastructure. Per application flow operations may be done at the demarcation point between the service provider and the customer, but inside the network, the granularity of traffic management is per customer or per service.

The details of access network QoS are discussed in much more detail in sections 3 and 4 of this document.

2.3. Public Network IP Voice Services

Despite all the hype that surrounds the Internet and IP, IP services are not yet significant contributors to the overall revenues of telecom service providers on a global scale. In 1999 legacy voice services generated more than 90% of service provider revenues worldwide. IP services (Internet Access, IP VPNs, mobile IP, etc.) were still in the low single percents (estimate 2-4%).

Voice will remain the highest revenue generating application throughout the five year scope of this paper. Therefore it is important to look at how voice services will be delivered from an IP infrastructure. Figure 2 presents the current PSTN architecture (with somewhat U.S. terminology). The PSTN is comprised of a hierarchical collection of TDM circuit switches. The end customers are either directly connected to end office switches (class 5 switches) or they are served from Digital Loop Carriers or remote switching units. In the U.S. market the DLCs typically connect to the switch using a standards based GR-303 or TR-08 interface. In the ETSI market the interface between the DLC (typically called remote switching unit or remote concentrator) is very often proprietary even though standards based V5.2 interfaces are also gaining popularity especially among the new competing operators.



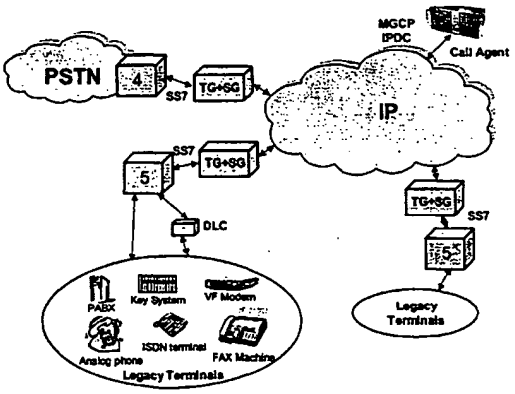
Legend	
DLC	Digital Loop Carrier
ISDN	Integrated Services Digital Network
LD	Long Distance
SS7	Signaling System 7
VF	Voice Frequency

Figure 2: Current PSTN Architecture

The current PSTN implements a huge amount of voice service functionality and presents a large capital investment, which cannot be replaced by IP solutions over any short time period. We believe that the circuit switched legacy voice network will keep on growing over the next five-year period. In the legacy voice networks, the role of

IP is limited to providing transport between TDM switching elements. All services are produced and all switching is executed using the TDM switches.

Even though the existing PSTN will dominate the voice service production over the next five years, IP based voice services will also grow over the whole five year period. IP voice will start generating significant revenues by the end of the five-year period. Some forward looking operators (read operators deploying in new territories without the burden of legacy infrastructure) will deploy IP based voice switching solutions during the first half of the five year period. Packet domain switching will first be implemented in the long distance voice network (class 4 switch replacement, see Figure 3) and later in the local networks (class 5 switch replacement, see Figure 4).

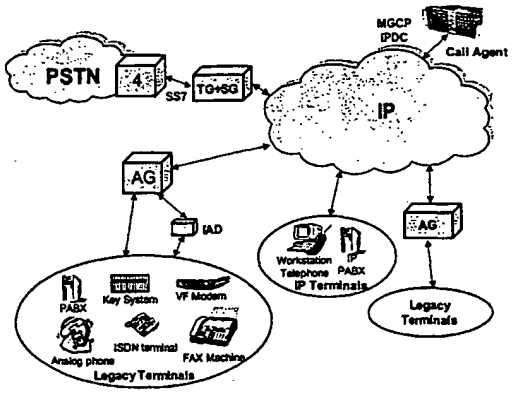


Legend	
DLC	Digital Loop Carrier
IPDC	Internet Protocol Device Control
ISDN	Integrated Services Digital Network
LD	Long Distance
MGCP	Media Gateway Control Protocol
PABX	Private Automatic Branch Exchange
SG	Signaling Gateway
SS7	Signaling System 7
TG	Trunk Gateway
VF	Voice Frequency

Figure 3: Class 4 switch replacement

In the class 4 switch replacement application the IP network looks like a collection of class 4 switches to the rest of the PSTN infrastructure. These types of architectures are being deployed today. One of the leading vendors in this space reported first quarter 2000 revenues of 1.1MUSD, which reflects the fact that this type of network architecture is still in the very early days. However, at least the analyst community expects this, and other IP voice architectures, to become a huge market since the market capitalization for the company mentioned above is more than 6BUSD (mid June 2000).

In the class 5 switch replacement scenario (see Figure 4), which actually is also class 4 replacement, the IP infrastructure replaces the end office switches and tandem switches within the reach of the managed IP network. The rest of the PSTN sees the IP network like it would see a class 5 or a class 4 switch.



Legend	
AG	Access Gateway
IAD	Integrated Access Device
IPDC	Internet Protocol Device Control
ISDN	Integrated Services Digital Network
LD	Long Distance
MGCP	Media Gateway Control Protocol
PABX	Private Automatic Branch Exchange
SG	Signaling Gateway
SS7	Signaling System 7
TG	Trunk Gateway
VF	Voice Frequency

Figure 4: Class 5 switch replacement

Figure 3 and Figure 4 reflect an important fact about the early deployment of public network IP voice services. The IP voice is implemented in a way where the IP network is made to replicate the functionality of the existing voice network. The mass of the existing voice applications and the existing customer premise equipment is so huge, that there is no way to introduce the IP network as a new separate service. Instead the IP infrastructure has to seamlessly integrate with the existing PSTN.

Once the IP networks gain a broader foothold, the next step is to start introducing new IP based services in addition to replicating the traditional PSTN functionality. At that point we will also start seeing significant numbers of native IP terminals as part of the customer premise equipment.

One important property of VoIP is the fact that it is very inefficient from a bandwidth point of view. In carrier networks the voice encoding schemes are typically limited to either G.711 64kbit/s PCM or G.726 32kbit/s ADPCM to be able to provide a MOS of 4.0 or better. A typical packetization interval is 10ms. This means that in a G.726

VoIP packet you end up having 40 bytes of voice and 40 bytes of IP+UDP+RTP headers. This means that the overhead is 100%. This may be acceptable in the core network, which is running over optics, but is definitely not economical in the bandwidth limited copper based access network. This inefficiency problem can be solved with header compression. There are link level header compression mechanisms already in existence and there is work in progress to define LSP level header compression and suppression mechanisms to allow efficient voice transport over MPLS (VoMPLS).

Public IP voice services set strict requirements to the delay the traffic can experience as it travels through the public network. The end-to-end delay for a voice call must be kept below 150ms one way (see ITU-T G.114).

The end-to-end delay consists of a fixed component and a variable component. The variable delay component is dominated by the contribution of queuing delays in the network elements. The queuing delay decreases as the link bit rate increases. It can be estimated that in three years the majority of core network links will be running at STM-4/OC-12c (622Mbit/s) or higher bit rates. At these rates delay is a relatively simple problem to handle.

Slow links (link bit rate below 34Mbit/s) are being used in the access networks. These links are typically based on transmission over copper cables. The vast majority of access lines in the world are currently copper based and this will not change in the next five years. DS1/E1 and DSL based links will dominate the access space. The control of latency on slow links requires link level fragmentation of large data packets. The fragmentation is specified in RFC 2686, "The Multi-Class Extension to Multi-Link PPP" [1].

Third generation mobile networks will also be an important contributor to the voice switching in the IP domain. Today the 3G specifications still have some amount of ATM content, but there is considerable effort being made to agree on an all IP architecture for these services. The real explosion of 3G services can be expected to commence towards the end of the five year period.

2.4. IP Data Services

The most popular data service will be Internet Access. This service will be ubiquitous in much the same way as current voice service offerings.

The Internet Access service will evolve from the current best effort service to a service portfolio supporting multiple traffic classes. We would expect that typically the number of service classes will be two (economy and business) but some operators will no doubt introduce additional classes.

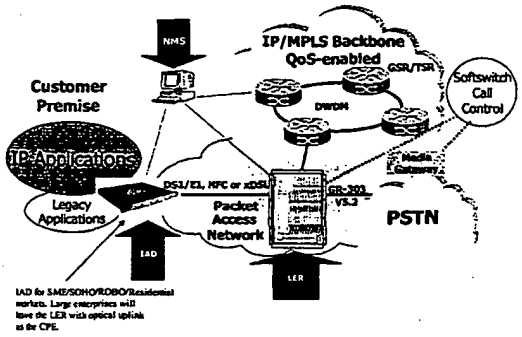
While Internet Access will be the highest traffic generator in the new public network, the largest data revenues will be generated by IP VPN services. These services will start replacing the current leased line and Frame Relay networks by the second half of the five year period.

Once QoS aware IP VPNs start getting deployed the distinction between a voice service and a data service is eliminated. The same IP fabric is used for switching both voice and data.

With a ubiquitous IP infrastructure and having virtually all applications running over IP, it becomes easy and economical to outsource various applications or IT functions. ERP application hosting, WEB based data storage and other ASP services are a big growth market. Even the voice service may become just another IP application in the soft-switch model with a voice ASP providing this service.

2.5. Next Generation Public Network

Figure 5 summarizes the architecture of the next generation public network.



Legend	
DS1	Digital Signal 1
DWDM	Dense Wavelength Division Multiplexing
E1	2048kbit/s according to G.703
GSR	Gigabit Switch Router
HFC	Hybrid Fiber Coax
IAD	Integrated Access Device
IP	Internet Protocol
LER	Label Edge Router
MPLS	Multi Protocol Label Switching
NMS	Network Management System
PSTN	Public Switched Telephone Network
QoS	Quality of Service
ROBO	Regional Office Branch Office
SME	Small and Medium Enterprise
SOHO	Small Office Home Office
TSR	Terabit Switch Router
xDSL	Digital Subscriber Line (x denotes either A for Asymmetric, S for Symmetric or V for Very High Bit Rate)

Figure 5: Future Network Operation

The legacy PSTN and new world IP/MPLS based network exist side by side. The backbone of the IP/MPLS network consists of high-speed routers, which are running on top of an optical DWDM core. The access is provided by an IP/MPLS enabled access network infrastructure.

The deployment of MPLS based access networks will lead to an end to end network with one homogeneous IP/MPLS based control plane. This means big savings for network operations since all the network layers can be managed using the same family of protocols. At the same time, new services can be created and rolled out more flexibly and faster.

The use of MPLS based access also allows LSP level header compression or suppression for voice, which is an absolute requirement to make VoIP over DS1/E1 based access economical.

3. QoS in IP/MPLS Networks

3.1. QoS classes required for new world IP applications

Before embarking on a discussion of a practical QoS implementation it is important to first define what is meant by QoS in the context of this paper. QoS is what the network operator promises his customers in an SLA, Service Level Agreement.

In an SLA the user and the operator agree on a traffic descriptor or the characterization of the traffic to be carried in the network. The operator gives a guarantee for the delivery of the traffic as long as the user stays within the agreed traffic profile (in practice the edge device of the operator ends up policing the user's traffic to make sure that it complies with the profile).

The traffic descriptor defines the bandwidth requirements and how bursty the traffic is. Given this description the network will guarantee delivery with a certain packet loss ratio, end-to-end delay and end-to-end delay variation.

Adjusting the absolute value of packet loss ratio or delay on a service by service basis is much too complicated to make any sense. Typically the goal for packet loss ratio is "effectively zero" packet loss. The absolute value for "effectively zero" depends on the service type.

In the case of delay it is again not realistic to try to adjust delay on a service by service basis. Instead the network needs to be built following certain design rules. The design rules together with the properties of the network elements will lead into certain maximum end to end delays. The same is true for delay variation.

Typically the Service Level Agreement would also include parameters like availability, MTBF and MTTR. These parameters are important to the QoS as the customer perceives it. High availability is delivered by having equipment and network level redundancy. Repair times are controlled with adequate monitoring and maintenance processes and resources.

The verification of conformance to SLAs requires advanced centralized management solutions capable of collecting statistics at LSP level and generating billing data and performance reports.

Today the largest data service revenues are generated by TDM leased line and Frame Relay services. In both of these service types the primary traffic parameter is the bandwidth. We believe that bandwidth will remain the most important traffic parameter as we transition to the IP based services.

The most popular data transport protocol today is Transmission Control Protocol, TCP. TCP is designed to operate over networks where the available bandwidth changes dynamically over time. A standards compliant TCP implementation tries to share the available bandwidth in a fair manner with other TCP sessions. An interactive TCP application needs some minimum bandwidth to give reasonable performance to the end user. Additional bandwidth will make the application run faster, but will not otherwise impact the operation of a well-designed application. Today's best effort Internet is a good match to the properties of TCP.

Another class of IP traffic is generated by real time applications, which do not tolerate packet loss or large delay. The bandwidth must be available when the application needs it and packets require timely delivery. Considerable effort is being spent on trying to develop new algorithms that will make real time applications adapt to the available bandwidth. However, it can be expected that there will always be applications that need guaranteed bandwidth and low delay.

To strike a balance between the complexity of implementation and the varying needs of different applications we propose that IP transport should be able to support four different traffic classes: Real Time (RT), Guaranteed (G), Guaranteed + Best Effort (G+BE) and Best Effort (BE).

RT-class will provide a guarantee for delay, delay variation and bandwidth. Delay and delay variation are typically expressed as network level constants and are not adjusted on a service by service basis. If the service spans large geographical areas, it may be necessary to have different zones for delay. However, the important point is that control of delay and delay variation is a result of network architecture and the specifications of network elements. Delay is not adjusted on an LSP by LSP basis.

G-class will give a bandwidth guarantee and may give some delay guarantee as well. Typically RT-class gives more strict delay and delay variation guarantees than the

G-class. Again the delay and delay variation guarantees are given at network (or at most zone) level and not on a service by service basis.

G+BE will guarantee a certain minimum bandwidth and allow the application to use more bandwidth on a best effort basis. This type of service class is a good match for TCP based applications. It assures the bandwidth necessary for acceptable application performance. In addition, any available excess bandwidth in the network can be shared by different services in a fair manner.

Finally the BE is the traditional Best Effort Internet service.

Operators need to give two kinds of bandwidth guarantees. Some applications will require strict end-to-end bandwidth guarantees. Any mission critical IP VPN services will fall into this category. If a production plant is accessing the ERP database over an IP VPN connection, an hour of low performance on this connection can easily cost more than the annual fee the operator charges the customer for the connection. For this application it is easy to see why the customer will only talk to an operator that promises high availability and guaranteed bandwidth.

One example of critical use of IP VPN service would be providing the connections to get the contents of a daily newspaper to the printing facilities. It is easy to see that this type of service has to be available and guaranteed over the critical early morning hours as the printing cannot tolerate any delays.

The other kind of bandwidth guarantee is for access bandwidth to the high speed IP backbone. In this model the operator guarantees certain bandwidth between the customer location and the core, but does not give any explicit bandwidth guarantees within the core. The treatment of the traffic in the core is defined by the DiffServ PHB that is assigned for the service. Note that if the traffic gets high enough priority in the core the end result may be guaranteed bandwidth end to end from the customer's premise to any destination within the IP backbone. The bandwidth in the core is managed by observing the actual usage and doing traffic engineering to keep the high priority traffic classes free of congestion. This requires a reasonable amount of excess bandwidth in the core to avoid ever running out of it. Naturally the excess bandwidth can be used for lower priority traffic classes, when it is not needed for the high priority service.

It seems unlikely that end-to-end bandwidth guarantees would be possible as a general rule over administrative domain boundaries within the five year scope of this document. The technical and contractual difficulties of implementing such services are so challenging that one can only expect a limited amount of such interoperability.

3.2. IETF Standards for IP QoS

IP QoS is defined in the IntServ and DiffServ working groups of the IETF.

The IntServ working group has specified an architecture for delivering per flow QoS end-to-end. The working group has specified three different service classes: Best Effort Service; RFC 2211, "Controlled Load Network Element Service" [2] and RFC 2212, "Guaranteed Quality of Service" [3].

The Controlled Load service is the same as the G-class mentioned in the previous section (see Table 1), if it is configured to drop any packets that exceed the token bucket specification.

	RT	G	G+BE	BE
Guaranteed	X			
Controlled Load		X	X	
Best Effort				X

Table 1: IntServ to RT/G/G+BE/BE mapping

The G+BE service class can be achieved by allowing the excess traffic to enter the network on a best effort basis.

Best Effort service naturally maps directly to the BE-class mentioned in section 3.1.

In most cases voice and other real time services require the use of Guaranteed Quality of Service as the Best Effort and Controlled Load services do not give any control over the delay. In practice the absolute delay bound given by the Guaranteed Quality of Service specification is not useful as it is far too pessimistic. The only useful piece of the delay specification is the qualitative information that delay is somehow bounded. The actual delay bound cannot be calculated using the formulas of RFC 2212 so a more practical approach is required.

The problem with the formulas of RFC 2212 is that they give an absolute bound to the delay. All packets will experience delay that is below the bound. In practice it is better to define an acceptable packet loss ratio, declare late packets lost and express the delay bound statistically. For example we might say that packet loss ratio of 10^{-5} is acceptable. Therefore we are only interested in delay bound for 99.999% of packets. If we further assume that the bandwidth utilization of the Guaranteed Quality of Service is below 100% we end up getting considerably lower delay values than the RFC 2212 formulas. See Figure 6 for a demonstration of the delay bounds (this figure is qualitative and not drawn to scale).

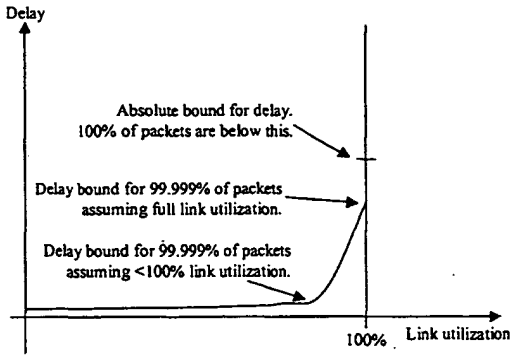


Figure 6: Queuing delay for real time traffic

The IntServ traffic parameters are token bucket rate r, peak rate p, minimum policed unit m, token bucket depth b and Maximum Packet Size M. Each flow is tested with a token bucket (see Figure 7) for conformance to the flow specification.

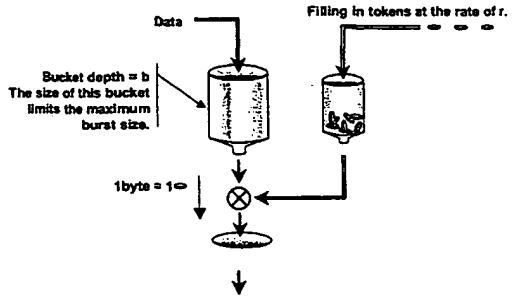


Figure 7: Token bucket

Routers on a path reserve enough resources (buffer space B and link bandwidth R) to provide zero packet loss and bounded delay to a flow that conforms to the token bucket.

It is important to note that the IntServ service classes were originally developed for per application flow QoS management. We do not believe that it is practical to try to manage QoS at application flow level inside the public network infrastructure. Instead the IntServ classes should be applied at LSP level.

Explicit resource reservations end-to-end are not practical in the WEB environment. Instead a relative or statistical approach to QoS is needed. The DiffServ working group of IETF has specified mechanisms for providing this type of aggregated QoS in combination with strict end-to-end guarantees. The DiffServ architecture is based on the idea that traffic is metered, shaped and policed at the edges of the DiffServ domain. Each packet is classified at the edge and marked with a DiffServ Code Point, DSCP. The core network elements treat packets based on these DSCP markings on a packet by packet basis. The different treatments a core element might give a packet are called Per Hop Behaviors or PHBs. The DiffServ working group has defined two new Per Hop Behaviors (PHBs): RFC 2597, "Assured Forwarding PHB Group" [4] and RFC 2598, "An Expedited Forwarding PHB" [5]. In addition the DiffServ specifications support best effort PHB and compatibility with the legacy IP TOS octet priority definitions.

The Assured Forwarding PHB is suitable for providing statistical QoS. It allows router resource allocation for up to four different AF classes. Within each class the user can define up to three drop priorities. The different drop priorities enable for example the olympic gold/silver/bronze service within the AF class.

The EF PHB is suitable for services which require strict end-to-end QoS. Note that the correct functioning of EF and the realization of strict end-to-end bandwidth and delay guarantees require adequate traffic engineering to keep the EF utilization on any core network link sufficiently low.

The DiffServ QoS model that is applied in the core of the internet, depends on the access network to meter, police and mark the traffic before handing it off to the core network. Unless sufficient traffic contract policing is done, the aggregated QoS in the core network will collapse.

4. MPLS Based Access Network Architecture

4.1. Requirements for the copper based access network

The key assumption we are making concerning the access network is that copper will be the dominant media in the access network over the next five years.

Bandwidth is not free even in the optical core, but it is especially scarce and expensive when running over a DS1/E1 or a DSL line.

This implies that accurate and strict traffic management is required in the access network to get the most out of the valuable resources.

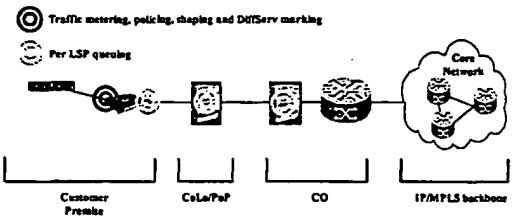
An absolute requirement in carrier class networks is that the service quality of one customer must not be impacted by the traffic load of another customer. In the core of the network, which typically runs over OC-48c links, it is virtually impossible for any single application flow or even any single customer to congest an entire link. Therefore DiffServ type per packet treatment which does not differentiate between customers or services is quite adequate. In the access network things are very different. On a DS1 line it is quite possible for one single application flow to congest the whole link. To isolate customers and services from each other and to provide maximum fairness

in sharing bandwidth between services, per service or per customer queuing is required. In an ATM network this translates into the requirement for per VC queuing. In an MPLS network this is called per LSP queuing.

Also, managing resources in core networks is much easier than in the access segment, since capacity shortages can be addressed by installing new 2.4Gbit/s links that vastly exceed the capacity of any single service. Meanwhile in the access network the addition of a single service can congest a network which had low utilization prior to adding the new service. The most efficient solution to this problem is the use of connection oriented transport and Call Admission Control for new connections. In ATM these connections are called VCs and in MPLS they are called LSPs. For the reasons mentioned in 2.2, we feel that the MPLS solution has significant advantages over an ATM based access network.

4.2. IP/MPLS Based Access Network Implementation

An MPLS based access system should consist of a customer premise IAD and central office Label Edge Router. In typical network architectures the traffic is groomed through one or two layers of the edge routers (see Figure 8).



Legend

CO	Central Office
CoLo	Collocation
DiffServ	Differentiated Services
IP	Internet Protocol
LSP	Label Switched Path
MPLS	Multi Protocol Label Switching
PoP	Point of Presence

Figure 8: MPLS Based Access Network Solution

All traffic is mapped into LSPs in the customer premise IAD and transported by LSPs to the CO node. The mapping of packets to LSPs depends on the content of the TCP, UDP and IP headers and sometimes even the content of the packet payload. All traffic management inside the access network is executed at LSP level and the system implements IntServ type QoS. The motivation for IntServ type QoS (rather than doing simple packet priority and DiffServ) is maximum efficiency of resource usage, maximum isolation of services that should not impact each other and maximum fairness among services that share common resources. See section 2.2 for a more detailed discussion on this subject.

The traffic contract for each LSP defines a peak information rate and a committed information rate. While it would be possible to also include the other IntServ traffic parameters (minimum policed unit m, token bucket depth b and Maximum Packet Size M) the use of system wide constants is recommended for these parameters.

The system supports four different traffic classes: Real-Time, Guaranteed, Guaranteed + Best Effort and Best Effort. These map to the four traffic classes discussed in the section 3.1.

The real-time traffic gets a delay guarantee. The delay guarantee is not based on the theoretical maximum limit as expressed by the formal "Guaranteed Quality of Service" specification. Instead the delay guarantee is a result of network planning rules. The maximum voice bandwidth utilization is limited to 92% of link bandwidth and the number of slow links (slow is defined to be anything slower than 34Mbit/s) on the path from customer premise to the central office is limited to two. The total number of links has to be below 8. The minimum link bit rate is a DS1 (1536kbit/s). The acceptable packet loss ratio for RT service is assumed to be 10^{-5}. This means a hit for modem or fax traffic once in 15 minutes at 10ms packetization interval. The service degradation for ordinary speech is unnoticeable at packet loss ratio of 10^{-5}. With these parameters the delay through the access network in one specific implementation can be guaranteed to be below 20ms.

It is also possible to plan the network so that the last mile is running at speeds lower than DS1. The minimum speed is 384kbit/s and the delay budget goes up by 5ms to 25ms in case the subscriber loop is running below the DS1 rate.

In ring architecture it is also possible to have more than 8 links in the access network. The delay budget needs to be increased by 0.5ms for each extra hop.

One of the main predictions made in the previous sections was that the core networks will be implementing DiffServ type QoS. Therefore it is very important for the access network to execute DiffServ marking and other DiffServ edge functions. The traffic conditioning and DiffServ marking of customer traffic are applied in the IAD, the traffic is carried through an LSP and handed of to the core as DiffServ marked IP or MPLS.

4.3. Traffic Management

The traffic management is based on an efficient implementation of token bucket + leaky bucket combination.

The key to this implementation is an efficient implementation of buffering and scheduling algorithms that closely estimate the ideal behavior of token bucket for

burst size policing and long-term rate limiting and leaky bucket for traffic shaping. This algorithm has been implemented with minimum processing overhead.

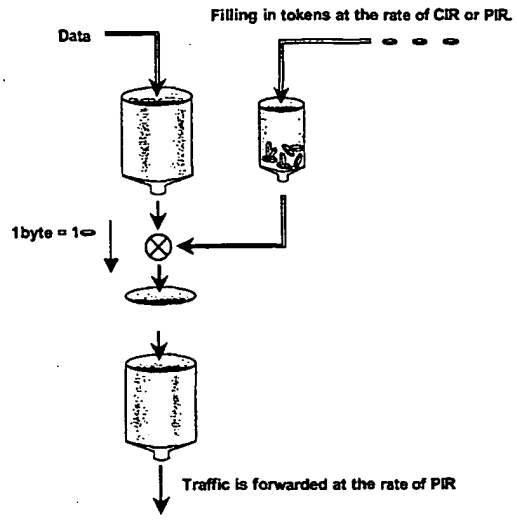


Figure 9: Token Bucket + Leaky Bucket

The system implements per LSP queuing as described in Figure 10. The bars in the middle of Figure 10 represent the amount of traffic (number of bytes) in the queue for each LSP. There is one queue for real-time traffic. Every G, G+BE and BE LSP gets its own queue. There is a token bucket + leaky bucket combination associated with each queue for draining the queue. LSPs within a service class (G, G+BE, BE) are served in a round robin manner and different service classes are served using priority queuing.

The per LSP queuing is executed at every hop inside the access network to reshape the traffic back to the original token bucket specification.

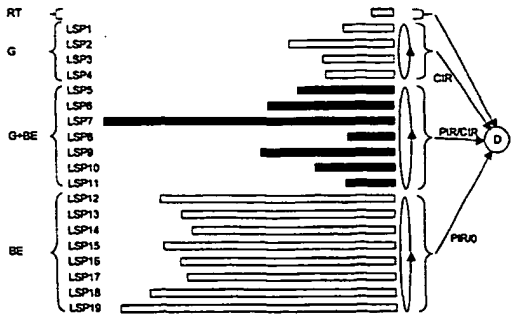


Figure 10: Per LSP Queuing

For G+BE traffic class the token bucket rate is PIR whenever the output interface is not congested. If the output interface gets congested, the token bucket rate is changed to CIR. This way the LSPs can run at peak rate for unlimited periods of time and only under congestion they are slowed down to CIR.

The G and G+BE classes are good implementations of the "Controlled Load Network Element Service". These traffic classes provides zero loss transport of traffic that conforms to the token bucket definition.

The real time traffic class provides an implementation of the "Guaranteed Quality of Service".

4.4. End-to-end IntServ services over a DiffServ core

From an IntServ point of view the interesting end-to-end services are "Controlled Load" and "Guaranteed".

"Guaranteed" service needs to be mapped to an EF DSCP to get a bounded delay in the network.

"Controlled Load" service can be mapped to an AF DSCP in such a way that traffic which conforms to the token bucket is marked with higher drop precedence than traffic which does not comply with the token bucket.

In the provisioning of IntServ services over a DiffServ core the key to guaranteed bandwidth and delay through the core network is the use of traffic engineering to keep the EF traffic class or the high priority part of the AF traffic class free of congestion on all core network links.

There are at least four possible ways of implementing such traffic engineering.

The simplest way is to limit the total amount of high priority traffic admitted to the DiffServ domain to be less than the link speed of the slowest core network link. This method can not be considered practical in production networks, which are trying to optimize the resource usage in the network.

A second method is to monitor the bandwidth usage on core network links and manually manipulate routing policies or carry out manual traffic engineering using MPLS whenever the bandwidth usage on a link exceeds an operator threshold. The amount of manual work implies that this method does not scale much better than the first method.

A third method is to deploy a centralized management system which manages the bandwidth in the core network links and configures the DiffServ edge traffic conditioners and routing policies or MPLS label switch paths to distribute the load optimally.

The best way to implement traffic engineering is to use MPLS for explicit routing of the traffic. The LSPs can be either calculated off-line by a management system or they can be routed based on an IGP (OSPF or IS-IS) which supports link resource information dissemination.

4.5. End-to-end DiffServ

Two approaches can be used for realizing end-to-end DiffServ services. Either the access network can be made to operate in DiffServ mode or the access network can be seen as providing guaranteed access to a DiffServ core.

The motivation for the latter approach is the fact that implementing AF with multiple drop precedence classes makes less sense when only a small number of customers is sharing the common resources.

4.6. Verifying service conformance to SLAs

The philosophy in MPLS based access network is to carry the traffic for each service over a dedicated LSP. Thus the performance of the LSP is the performance of the service.

The access network solution needs to be augmented by an advanced management solution, which collects performance and accounting statistics at LSP level. The NMS should capable of generating both accounting data for usage based billing and performance data for SLA conformance monitoring.

5. Conclusion

Core networks are converging towards IP/MPLS over optics architecture. Therefore the most natural and logical fit for an IP based core network is an IP/MPLS based access network.

To support the integration of both voice and data services the access network needs to implement per LSP traffic management and the IntServ service classes.

Since QoS in core networks will be based on DiffServ, both interworking for delivering end-to-end IntServ services over a DiffServ core and providing end-to-end DiffServ services need to be defined.

6. References

[1] : IETF RFC 2686, Bormann, The Multi-Class Extension to Multi-Link PPP, September 1999.

[2] : IETF RFC 2211, Wroclawski, Specification of the Controlled-Load Network Element Service, September 1997.

[3] : IETF RFC 2212, Shenker, Partridge, Guerin, Specification of Guaranteed Quality of Service, September 1997.

[4] : IETF RFC 2597, Heinanen, Baker, Weiss, Wroclawski, Assured Forwarding PHB Group, June 1999.

[5] : IETF RFC 2598, Jacobson, Nichols, Poduri, An Expedited Forwarding PHB, June 1999.

Hybrid Transport Solutions for TDM/Data Networking Services

Enrique Hernandez-Valencia, Lucent Technologies

ABSTRACT

There is a growing demand for native data transport services for enterprises and corporations across public transport networks. Recently, equipment vendors have begun to incorporate a variety of LAN and storage area network interfaces, notably Ethernet, Fibre Channel/FICON, and ESCON, on traditional metro and long-haul transport equipment. Embracing Ethernet and SAN technology enables the introduction of flexible high-capacity transport services optimized for data networking. Transport operators may thus offer both enterprise-centric connectivity services, such as transparent LAN connectivity and virtual LAN services, as well as traditional bandwidth services, such as private lines, while preserving the operations and management infrastructure of the existing public networks. In this article we discuss the benefits of a hybrid Ethernet/TDM transport solution.

INTRODUCTION

With the onset of the information age, a wide variety of specialized connectivity, storage, content, and data distribution/processing services have sprung across the telecommunications/data communications landscape. These services vary from traditional telephony and private line connectivity services over the public switched telephone network (PSTN) infrastructure, to virtually switched circuits for WAN data networking (from most major telecommunications carriers), also to IP-oriented virtual private networks (VPNs) and residential/business Internet access services offered by Internet service providers (ISPs), and also to a new breed of Web hosting/storage and information processing services offer by application/storage service providers (ASPs/SSPs).

In order to address the need for connectivity, capacity, and content arising from the information age, service providers are quickly converging to a new view of the telecommunications and data communications business. Connectivity, capacity, and information services are each dealt with as one of the various services to be supported by a common public transport infrastructure. The relentless growth in bandwidth, connectivity, and content demand fueled by the Internet revolution has made bursty information transfer the main application driver of modern communications systems. As the packet switching technology that constitutes the basis of modern data communications networks matures, opportunities for integration with the common transport, multiplexing, and switching functions within the public transport infrastructure become more clearly defined. Fibre Channel, FICON, and ESCON are the most prevalent technologies deployed for storage networking. Ethernet is the de facto enterprise network standard for data communications. Extending enterprise and data center connectivity over the metro access/core network infrastructure is an obvious first step in deploying connectivity services over traditional transport networks. This new emerging paradigm is illustrated in Fig. 1. The transport network is multiservice. It enables a variety of basic connectivity services for both circuit and data applications over native data interfaces. Sophisticated data and content services that require finegrained per-user control are delegated to an intelligent services layer. For this services layer the transport network provides traditional traffic aggregation and distribution services on a wholesale basis.

SERVICE CONVERGENCE AS DRIVERS FOR HYBRID TRANSPORT SYSTEMS

The increased multiservice nature of a converged transport network infrastructure requires efficient handling of narrowband, wideband, and broadband traffic sources whether from voice, Web pages, electronic data exchanges, packetized digital audio, or video. Furthermore, service providers demand an enduring public transport network infrastructure that provides a flexible and affordable service evolution path despite unpredictable traffic patterns, service models, and technology evolution. Revenue generating services (e.g., private lines) must be preserved at the same level of expectation for survivability, manageability, and maintenance.

0163-6804/02/$17.00 © 2002 IEEE

One trend toward a converged public transport network evolution is to convert every transport node in the public transport infrastructure into a packet switching device. Such an approach is attractive to greenfield operators, to smaller metro-oriented carriers with no other embedded communications infrastructure (e.g., metro C-LECs), or to new entrants with a highly specialized portfolio of services (e.g., E-LECs). This approach has turned out to be more complicated than initially envisioned given the configuration, operations, and management complexity associated with most packet-switched services, the relatively high cost of deployment of such an integrated services transport paradigm over the public switching/cross-connect facilities, and the narrowly focused customer base. It also carries a higher degree of uncertainty given the desirability to support profitable telecom services such as voice and private lines, and the relative immaturity of such transport services over packet-switch-centric technologies (other than asynchronous transport mode, ATM [1]).

Another trend is to include packet transport, multiplexing, and switching capabilities on synchronous optical network (SONET)/synchronous digital hierarchy (SDH) add/drop multiplexers (ADMs) and broadband crossconnect systems (BXCs). The goal here is to incorporate basic packet transport capabilities that help enable packet-oriented connectivity services over the existing transport infrastructure rather than on a fully collapsed transport, services, and applications layer. (For such an approach there are already well-defined transport mechanisms, e.g., ATM). Such an integrated TDM/data transport approach is attractive to established carriers as they can deploy new packet-switching technology to implement data transport services on an as-needed basis. It also facilitates the controlled introduction of operations, administration, management, and provisioning (OAM&P) procedures for those new services, and reuses the existing transport capabilities of deployed TDM networks.

Emergency of Ethernet Transport Services

Over the last few years we have seen Ethernet emerge as the dominant technology for LANs and enterprise networking. Ethernet has also begun to make inroads as a networking solution for storage facilities in corporate/hosting collocated data centers, and as an interconnect solution among ISP points of presence (POPs) in metropolitan networks. Among the drivers for Ethernet's popularity are its relative simplicity, maturity, and volume of sales (with corresponding lower manufacturing costs), particularly for short/medium reach data connections (up to a few kilometers). For example, compared to traditional packet over SONET/SDH (POS) interfaces, Ethernet interfaces can be as much as 50–80 percent lower in price (albeit with more limited OAM&P capabilities than typically required by public-grade telecommunications services). For best effort and non-mission-critical traffic, which dominates most corporate/enterprise data traffic today, TDM and ATM networks provide a level of performance, reliability, and service features beyond that required by these applications. Ethernet-based solutions, particularly on the access portion to the MAN, can fulfill this particular end user's needs.

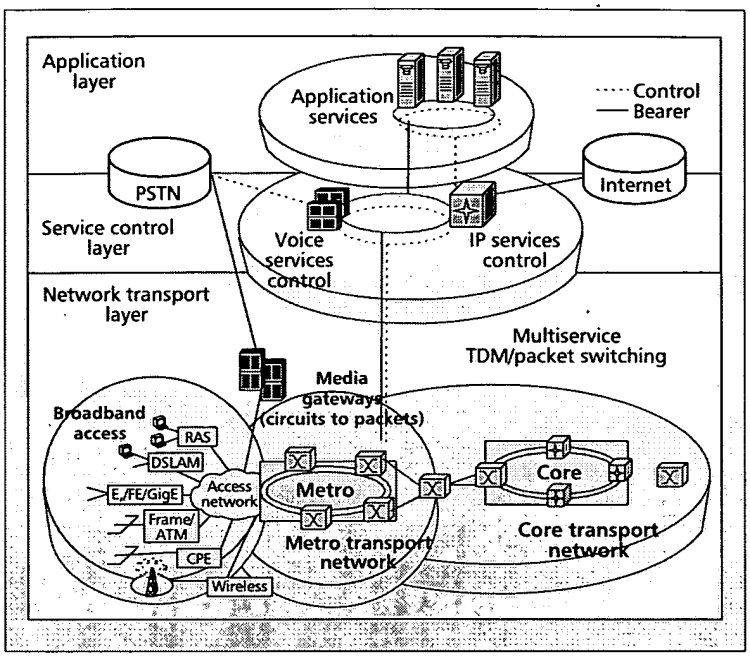


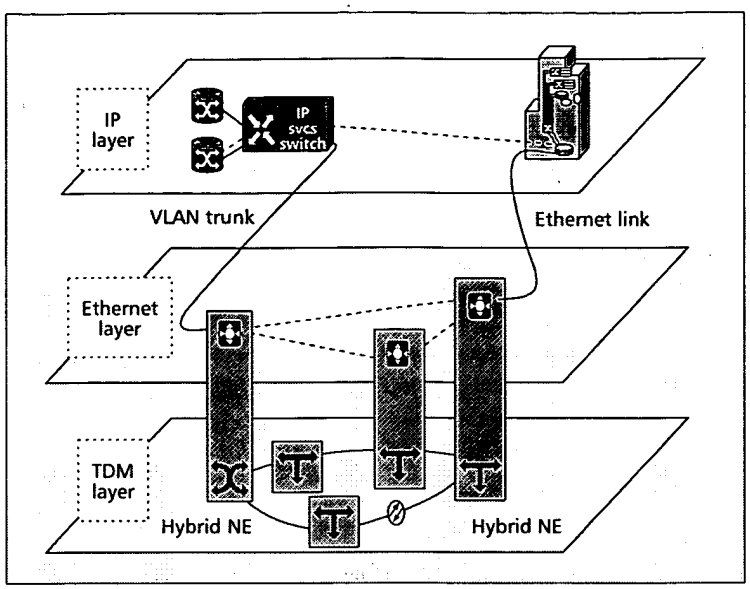
Figure 1. *The emerging converged network model for public transport networks.*

Networks built upon SONET/SDH and wave-division multiplexing (WDM) are optimized for delivery of reliable cost-effective transport for voice, private line, and other mission-critical services that continue to dominate the access network revenue stream today. However, pure SONET/SDH and WDM networks are not yet optimized for addressing all the data transport needs. For instance, it has not been until recently that TDM solutions have been enhanced with flexible traffic aggregation and multiplexing mechanisms, or the granular bandwidth allocation schemes required for data communications. These shortcomings related to data transport have begun to be addressed with next-generation hybrid network architectures.

A Layered Hybrid Network Architecture Model

A recent development in service convergence is to integrate Ethernet technology into public transport networks. Support for standard Ethernet interfaces directly on network elements such as SONET/SDH ADMs/BXCs and dense WDM (DWDM) optical line systems (OLSs) enables native service interfaces for data transport. This approach exploits low-cost data interconnectivity on the enterprise equipment while maintaining the reliable and manageable transport infrastructure required in large public networks. We refer to this technology as *hybrid transport*.

Figure 2 depicts the functional layering model of the data transport capabilities in a hybrid Eth-



■ **Figure 2.** *The layered TDM/Ethernet transport model.*

ernet/TDM architecture. At the bottom of the hierarchy is a standard transport network, consisting of SONET/SDH ADMs and BXCs, that supports traditional time-division multiplexed (TDM) services such as voice and private lines. Incorporated into these network elements are Ethernet/IEEE 802.3-based connectivity [2], IEEE 802.1D/w [3] bridging functions, as well as IEEE 802.1Q/p-based virtual LAN (VLAN) network services and QoS capabilities [4]. These features facilitate the logical overlay of data-aware unicast, multicast, and broadcast transport services currently not available over a SONET/SDH network infrastructure. In this manner the transport network can easily be configured, and enhanced, to offer not only native data interfaces but also native transport service already familiar to the data communications community.

A number of new data transport services can now be offered to enhance the operator's revenue stream. Sample services include virtual leased lines and Ethernet-based virtual private networks (VPNs). The implementation model for these services is discussed later.

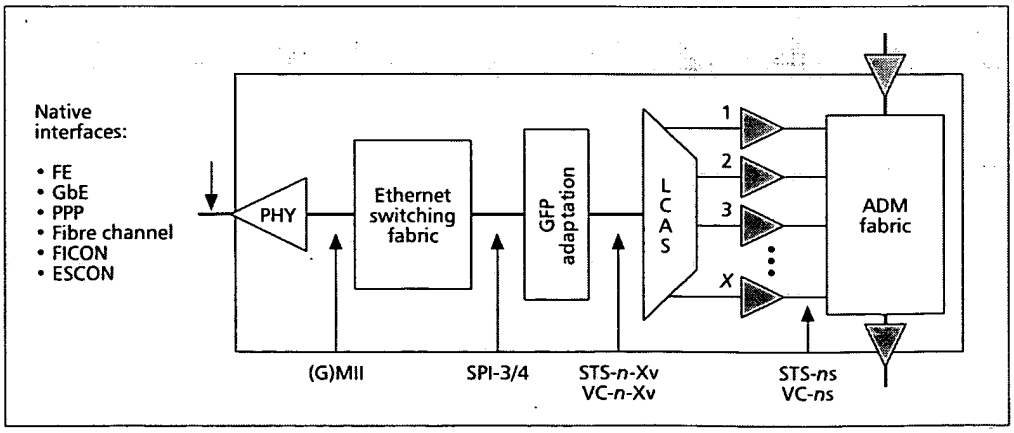
Enabling Ethernet Transport over SONET/SDH

Three key technologies help enable storage networking and Ethernet transport over SONET/SDH networks: virtual concatenation of SONET/SDH paths, virtual bandwidth allocation via the Link Capacity Adjustment Scheme (LCAS), and the Generic Framing Procedure (GFP) to adapt the MAC frames (e.g., the IEEE 802.3/Ethernet frames) to the octet synchronous SONET/SDH payload. A functional view of such a hybrid TDM/Ethernet network element model is illustrated in Fig. 3. How these three mechanisms interwork to support the implementation of data transport over SONET/SDH is discussed next with a focus on Ethernet solutions. The same concepts can be extrapolated to storage networking.

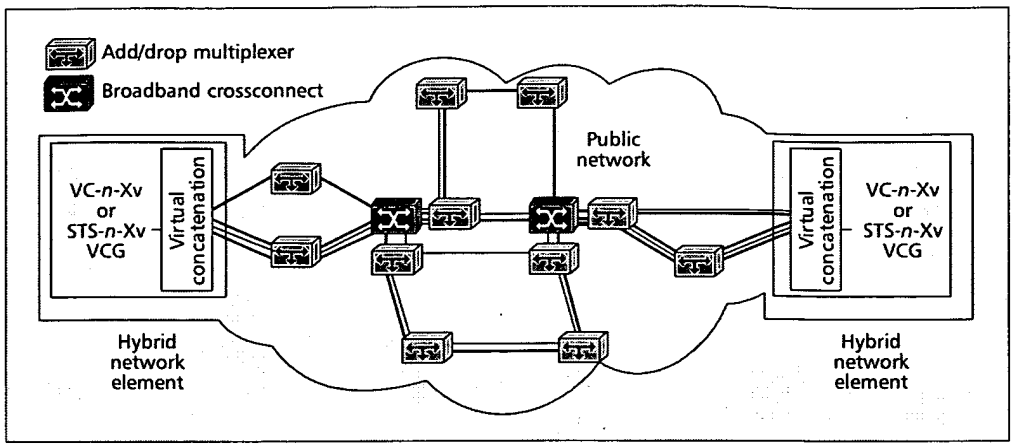
Virtual Concatenation

SONET/SDH systems were initially optimized for the transport of telephony services. Given the constant bit rate (CBR) nature of voice and private line traffic, a coarse fixed-rate multiplexing hierarchy was most efficient for the transport of these CBR signals. Data traffic, however, is inherently bursty. The bulk of this traffic demands elastic bandwidth allocation. This demand can easily be accommodated with a best effort delivery service. Statistical multiplexing, via packet switching technologies, provides far better utilization of the transport medium for this type of applications. Neither the signal rate nor the nominal data rate of popular physical interfaces for data networks makes efficient use of the existing SONET/SDH channel sizes. A flexible mechanism to interact with the SONET/SDH multiplexing hierarchy was required.

Virtual concatenation [5, 6] is an inverse multiplexing technique that combines an arbitrary number of SONET/SDH transport channels to create a single-octet synchronous byte stream. It is an alternative to standard contiguous concatenation, which only supports aggregation and multiplexing in $4^N \times$ STS-3cs (SONET) or $4^N \times$ VC-4 (SDH) containers. With virtual concatenation, network operators can bundle an arbitrary number (X) of either low-order (e.g., VC-12s or VC-3s in SDH or VT1.5s in SONET) or high-



■ **Figure 3.** *The hybrid ADM/Ethernet network element model.*



■ **Figure 4.** *Transport of constituent VCG components over SONET/SDH.*

LCAS is an extension to virtual concatenation that allows dynamic changes in the number of SONET/SDH channels in a connection under management control of the initiating/terminating network elements such that hitless performance of the VCG is guaranteed.

order (e.g., VC-4s in SDH or STS-1s/STS-3cs in SONET) channels to create a single virtual concatenation group (VCG) signal (e.g., VC-12-Xv/VC-3-Xv/VC-4-Xv in SDH or VT1.5-Xv/STS-1-Xv/STS-3c-Xv in SONET). An important aspect of virtual concatenation is that the individual transport paths that constitute the VCG can be transported independently over the SONET/SDH network. As illustrated in Fig. 4, only VCG initiating/terminating equipment at the edge of the transport network (typically implemented in a line card) needs to support this function. Virtual concatenation works seamlessly with legacy SONET/SDH equipment. The rest of the transport network simply transports the component TDM channels independent of each other. In addition, virtual concatenation provides mechanisms to manage not only the constituent paths of the VCG, but also compensation for the differential delays among those paths across the SONET/SDH network. Thus, virtual concatenation addresses bandwidth allocation constraints associated with the coarse multiplexing hierarchy of traditional SONET/SDH systems.

With virtual concatenation bandwidth can be allocated as needed to accommodate the precise bandwidth requirements of the end systems. For example, an enterprise might need a 100 Mb/s Ethernet pipe to interconnect sites in a given metro area. This task can be accomplished by allocating either 2 STS-1 channels (SONET) or VC-3 channels (SDH), and then combining these two channels into a single VCG as a VC-3-2v byte stream of roughly 2*48 = 96 Mb/s. This is s substantial improvement, about 33 percent, over allocating a conventional VC-4 path at roughly 155 Mb/s for the same purpose, and hence without the associated waste of the unused channel capacity. The local connection at the enterprise site can be done with conventional Fast Ethernet interfaces.

Better yet, virtual concatenation affords network operators with a new mechanism to provide value-added connectivity services, such as fractional or subrate Ethernet transport services. Here, enterprises may attach to the transport network with an inexpensive short-reach Gigabit Ethernet interface. However, customers may only request enough transport capacity to meet the anticipated interoffice traffic volume, say 150 Mb/s. The network operator may configure such service by only allocating a single VC-4 or 3 STS-1s to the associated VCG between the two sites. When demand goes up, the enterprise may request that the capacity of the VCG be upgraded, say in VC-4 or STS-1 increments, until the 1 Gb/s limit is reached for the available GigE interface (and assuming the additional transport resources are available).

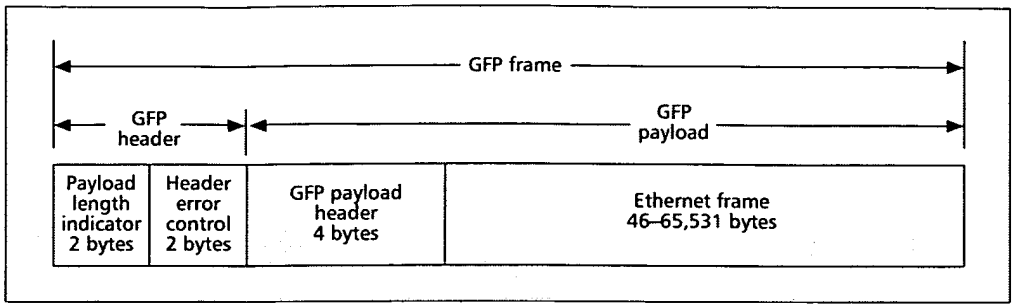
Link Capacity Adjustment Scheme

Modifying VCG size by adding or removing constituent channels may render the data path useless if proper coordination among endpoints is not provided. LCAS [7] is an extension to virtual concatenation that allows dynamic changes in the number of SONET/SDH channels in a connection under management control of the initiating/terminating network elements (NEs) such that hitless performance of the VCG is guaranteed. LCAS also allows dynamic removal (addition) of failed (recovered) constituent paths. Channels can be added or removed by management actions while in service. The VCG capacity modifications will occur without scheduling any facility downtime to reconfigure the data service and without losing any customer traffic.

VCG/LCAS provides the equivalent of an intelligent link aggregation facility for SONET/SDH much in the same way the IEEE 802.3ad specification provides link aggregations facilities for Ethernet segments. It also allows the implementation of connectivity services with graded levels of performance, (e.g., higher transport throughput when there is no failure in any of the constituent channels). When there is a failure in one of the constituent channels, the available bandwidth will be lower without incurring complete failure of the transport service. This is achieved by ensuring that only the failed channels of the VCG are withdrawn from service while the remaining channels will continue carrying live customer traffic.

The VCG/LCAS approach is advantageous for QoS transport services such as DiffServ for IEEE 802.1Q/p VLANs or IP/MPLS networks [8]. In such networks, packets are appropriately

Virtual concatenation by itself is not sufficient to create a transport link that fits the exact bit rate of the native data signal into the SONET/SDH payload areas. A mechanism is still needed to map the native bitstream into the SONET/SDH channel, providing for signal rate adaptation and minimal OA&P functions.



■ **Figure 5.** *The frame format for Ethernet over GFP using a null extension header.*

classified and marked to reflect different levels of handling priority with respect to packet loss and resiliency. An IP router or Ethernet VLAN switch will notice that less bandwidth has become available on an LCAS-enabled link experiencing a channel failure event. If temporary congestion arises from such an event, only the traffic with lower handling priority would be affected. In addition, for IP-based networks, the logical network topology need not be affected by such a change because IP-level connectivity is still maintained. Therefore, IP routing protocols do not need to reconverge; hence, no service interruption occurs.

In addition, traditional SONET/SDH protection schemes for highly reliable transport services may still be enabled. These are implemented as top-quality protection services over the SDH/SONET or WDM layer. They further allow service providers to offer graded levels of protection services and treat different traffic sources according to their revenue cost structure.

Transporting Packets in Circuits: The Generic Framing Procedure

Virtual concatenation by itself is not sufficient to create a transport link that fits the exact bit rate of the native data signal into the SONET/SDH payload areas. A mechanism is still needed to map the native bitstream into the SONET/SDH channel, providing for signal rate adaptation and minimal OA&P functions. The Generic Frame Procedure (GFP) fulfills this role. GFP is a lightweight adaptation protocol that provides a flexible mechanism to map different bitstream types to an octet-synchronous channel. The adaptation mechanism is frame-based and allows the segmentation of the physical channel into fixed or variable size containers, GFP frames. Two modes of signal adaptation are provided with GFP.

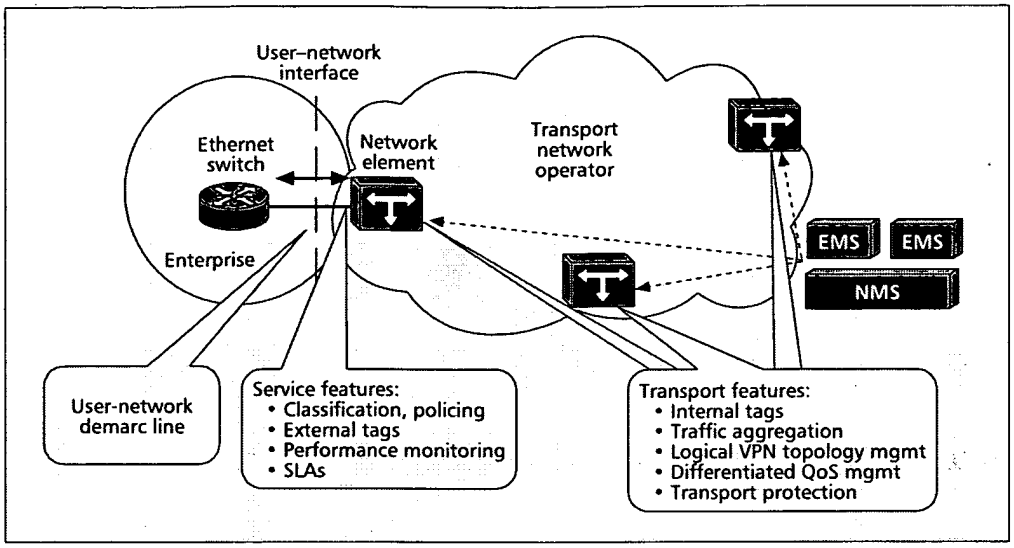
The transparent-mapped adaptation mode (currently defined for 8B/10B encoded signals only) is particularly suitable for full-rate point-to-point applications. (By full-rate is meant that the entire capacity of the local physical interface is supported). Adaptation is accomplished by mapping link-layer codewords into GFP frames. This mode is intended for applications that seek to emulate a native physical interface with very strict packet delay, loss, and throughput requirements (e.g., Fibre Channel, FICON, and ESCON).

The frame-mapped adaptation mode is a more flexible adaptation mode that is suitable for either full-/subrate point-to-point and multipoint applications. Adaptation is accomplished by mapping upper-level protocol data units (PDUs), such as Point-to-Point Protocol (PPP) frames or IEEE 802.3 MAC frames, rather than link-layer code words, into the GFP frames. The frame structure for mapping an Ethernet/IEEE 802.3 frame on a GFP frame (assuming a null extension header) is illustrated in Fig. 5. For applications where both the transport and bridging capabilities of Ethernet are integrated into the transport NEs, the frame-mapped mode is the preferred mode of adaptation since the physical layer aspects of both the SONET/SDH and Ethernet interfaces (layer 1) are segregated from the media access control (layer 2) aspects. Since the same mode of adaptation is applied to either point-to-point or multipoint configurations, service providers can deal with these two styles of application with the same provisioning and management procedures. Thus, for instance, if a customer wishes to migrate from a point-to-point transport service to a multipoint transport service, both of these services can be delivered from the same service interface without further reconfiguration of the preexisting endpoints.

Although many proprietary mechanisms abound for adaptation of native data traffic into SONET/SDH channels, GFP is the only international standard supported by both the American National Standards Institute (ANSI) and International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) [9]. GFP is a highly efficient encapsulation protocol with a fixed, but small, overhead per packet. Unlike most framing protocols, GFP scales very well to higher transport rates, which is one of the reasons GFP is being widely adopted for various high-speed applications such as optical channels in ITU-T optical transport network (OTN) architecture [10].

Hybrid Ethernet Transport Services

Based on the transport enhancements to SONET/SDH aggregation and multiplexing just described, new data-centric connectivity services can easily be instantiated over the public transport network infrastructure. Basic hybrid Ethernet transport services can be classified, in terms



■ **Figure 6.** *A reference model for services over the public transport network.*

Ethernet private line (EPL) refers to the simplest of the Ethernet connectivity services. It offers point-to-point connectivity between two remote sites by emulating the transport service delivered by an Ethernet segment, but over the public transport network.

of transport feature complexity, into three generic groups, namely:

- Ethernet private line services
- Transparent LAN interconnect services
- Access to managed IP services

Below we highlight service and transport features that can be associated with those services. For the purposes of discussing these services it is useful to think of the transport network as a black box. The network elements must distinguish between end-user and network transport services. End-user service attributes cover service characteristics negotiated between the customer and the service provider (typically using a user-network signaling or management interface). Transport network services cover service attributes that are based on well-known transport and networking mechanisms, and enable the delivery of the contracted services according to negotiated service level agreements (SLAs). All traffic management capabilities would reside on this layer, and any sophisticated QoS mechanisms would be implemented on the packet-switching components of the NE. Initially such end-user and network transport services and features may be configured via element/network management systems (EMS/NMS). Such a view is illustrated in Fig. 6. In the future, it may be possible to request such services and features via a well-defined user–network interface. Efforts in that direction are already underway in the Metro Ethernet Forum.

Ethernet Private Lines

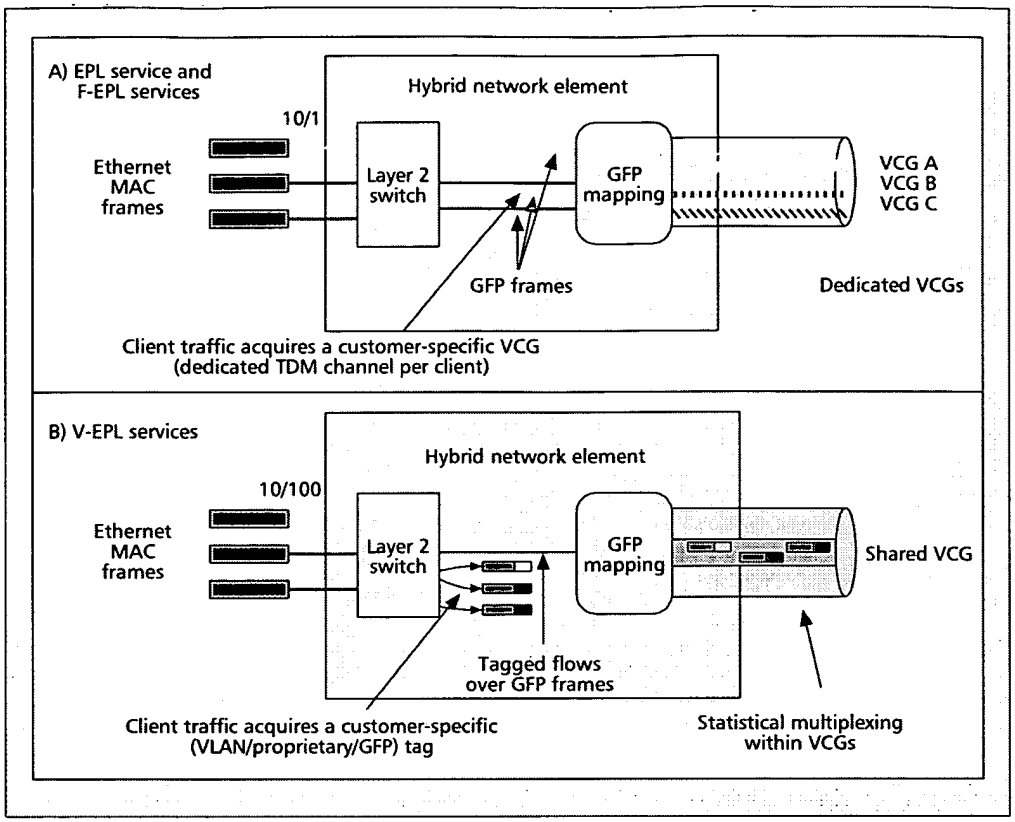
Ethernet private line (EPL) refers to the simplest of the Ethernet connectivity services. It offers point-to-point connectivity between two remote sites by emulating the transport service delivered by an Ethernet segment, but over the public transport network. This is a particularly useful service that can be used to extend the distance limitations of standard 10/100 Mb/s and 1 Gb/s Ethernet interfaces by reusing the connectivity services delivered by SONET/SDH paths over metro and long-haul networks. Such an approach would be substantially more efficient and cost effective than traditional solutions based on deploying optical transponders at both ends of dedicated lateral fibers to interconnect the end-user sites to the operator's infrastructure. The cost of the equipment and fiber access infrastructure is shared across multiple end users.

In the past transport of native Ethernet signals on SONET/SDH proved inefficient due to the capacity mismatch between the nominal signal (or

Traffic type	SONET		SDH	
	Contiguous	Virtual	Contiguous	Virtual
10 Mb/s Ethernet	STS-1 (20%)	VT-1.5-7v (89%)	VC-3 (20%)	VC-12-5v (92%)
100 Mb/s Fast Ethernet	STS-3c (67%)	STS-1-2v (100%)	VC-4 (67%)	VC-3-2v (100%) or VC-12-46v (100%)
200 Mb/s (ESCON)	STS-6c (66%)	STS-1-4v (100%)	VC-4-4c (33%)	VC-3-4v (100%) or VC-4-2v (66%)
1 Gb/s (FC/FICON)	STS-21c (85%)	STS-1-18v (95%)	VC-4-16c (35%)	VC-4-6v (95%)
1 Gb/s Ethernet	STS-24c (83%)	STS-1-21v (95%)	VC-4-16c (42%)	VC-4-7v (95%)

■ **Table 1.** *Transport efficiency of contiguous vs. virtual concatenation transport of Ethernet private line services over SONET/SDH.*

The simple EPL service model over a dedicated TDM transport channel supporting the peak interface rate can be enhanced in various ways to deliver a variety of value-added Ethernet connectivity services. As a starting point, operators may choose to support Ethernet transport services at subrates of standard 10/100 Mb/s and 1 Gb/s access interface rates.



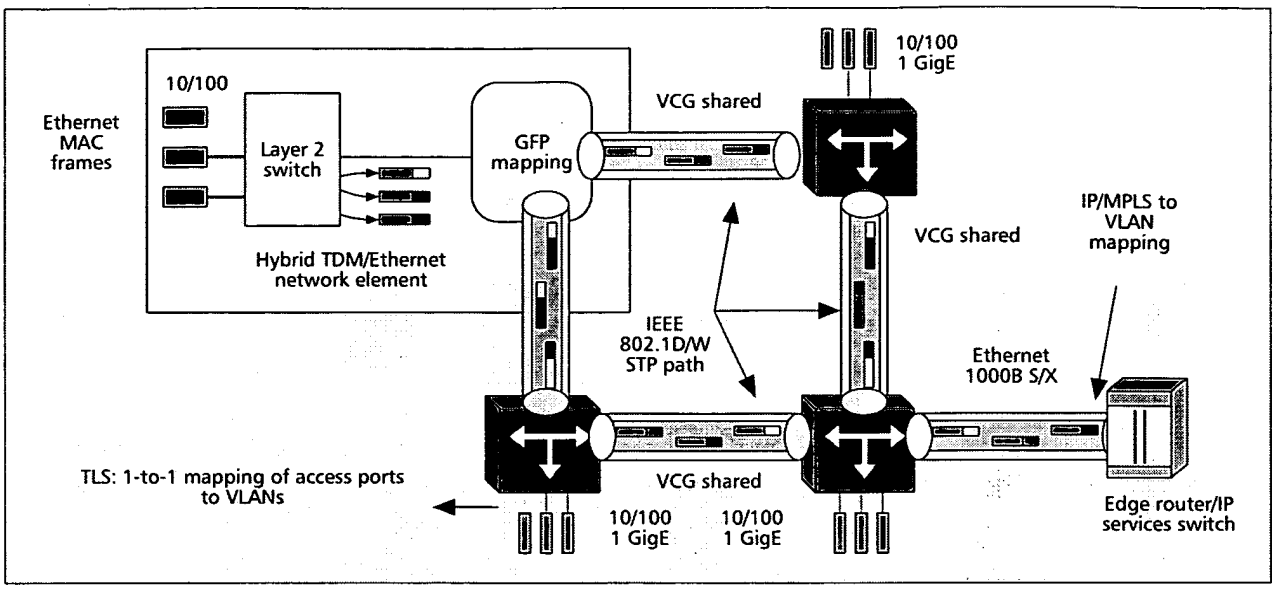
■ **Figure 7.** *Ethernet private line services (EPL, F-EPL, and V-EPL) over TDM channels.*

data) rates and the capacity of the SONET/SDH payload. This packing inefficiency is shown in Table 1. For instance, transporting a 100 Mb/s signal over a contiguously concatenated STM-3c/VC-3 would only result in 67 percent transport efficiency, that is, 50 Mb/s would be wasted for each 100 Mb/s connection. Virtual concatenation and GFP help address these past limitations in SONET/SDH payload granularity by providing transport containers closer to the nominal data rate and a low overhead mapping mechanism of the MAC frames into the SONET/SDH payloads. For the case of 100 Mb/s EPL, efficiency in the nominal data rate is close to 100 percent. (Note that these numbers assume the elimination of interpacket gaps, IPGs, which provides another 3–5 percent gain in efficiency for Ethernet payloads. They do not include bandwidth allocation for service management functions.)

Figure 7a illustrates a typical instantiation of EPLservices over a hybrid SONET/SDH network element. Each user flow is allocated to a segregated TDM channel. The TDM channel itself is composed of multiple STS-Nc/VC-N paths virtually concatenated into a VCG (VCGs A, B, and C in Fig. 7a). Each VCG would be sized to meet specific end-user requirements as specified in an SLA (typically the full capacity of the access line rate).

Fractional and Virtual Ethernet Private Lines — The simple EPL service model over a dedicated TDM transport channel supporting the peak interface rate can be enhanced in various ways to deliver a variety of value-added Ethernet connectivity services. As a starting point, operators may choose to support Ethernet transport services at subrates of standard 10/100 Mb/s and 1 Gb/s access interface rates. Such services are useful for enterprises that generate long-term traffic demands at a fraction of the links' peak rate. A fractional Ethernet private line (F-EPL) service can easily be implemented by configuring the transport path at a fraction of the access link rate. Typically, the path is configured at either VT1.5/VC-12 (1.5 Mb/s), STS-1/VC-3 (50 Mb/s) or STS-3c/VC-4 (150 Mb/s) granularity using standard virtual concatenation procedures.

Furthermore, operators may choose to configure arbitrarily sized transport paths and share the TDM capacity across multiple such F-EPL users. This approach allows service operators to achieve further transport efficiency via statistical multiplexing and graded levels of performance. Such virtual EPLs (V-EPLs) can easily be implemented using either GFP-based tags, such as those from the GFP linear extension header, IEEE 802.1Q/p VLAN tags (assuming these tags are not already in use by the end systems), or stacked VLAN tags by tagging the different flows with IEEE 802.3Q-compatible VLAN tags as illustrated in Fig. 7b. These features allow differentiated traffic treatment and QoS that can be indicated via the IEEE 802.3 user priority field. Note, however, that these services do require additional transport overhead for the virtual link identifiers that need to be accounted for as part of the traffic engineering requirements.



■ **Figure 8.** *Access to managed IP services via transparent LANs (over shared TDM channels).*

F-EPL and V-EPL services are intrinsically bursty packet-switched services that exploit the gaps in the end-user flow for statistical multiplexing gain. This style of service presumes at least a minimal set of resource management capabilities integrated into the transport network element (above the SONET/SDH transport layer) to help a service operator meet QoS commitments. QoS-based packet scheduling (e.g., Strict Priorities, Class Based Queuing, or Weighted Fair Queuing) and active queue management (e.g., Random Early Discard, RED, Band Weighted RED), typically not subject to standardization, are required. Other traffic management mechanisms may include flow control across the UNI via mechanisms such as IEEE 802.3x (Pause Frame) or shaping/policing of the user flows according to a committed information rate (CIR)/peak information rate (PIR).

Transparent LAN Interconnect Services

With the growing need to share resources across multiple enterprise sites over larger and larger distances, many enterprises find themselves faced with the need to interconnect their LANs using either private or public transport facilities. Often LANs are connected via a dedicated private line circuit (e.g., T1/E1s, DS3/E3s, or *n*64 kb/s) or packet switching technologies like X.25, frame relay, and ATM. These solutions are traditionally optimized for unicast services, and based on transport solutions different from the LAN technology prevailing in the enterprise environment that provide both unicast and multicast transport services. To address this limitation, it is simpler to integrate not only the Ethernet physical interfaces directly onto the network transport equipment, but also the media access control (learning and bridging) capabilities.

Transparent LAN services thus refer to a generic set of transport features that enable multipoint connectivity services to extend Ethernet learning and bridging functions over the public transport network. These services facilitate sharing of enterprise/corporate resources over metro access/core networks by emulating the transport services offered by the Ethernet/IEEE 802.3 MAC layer.

Multiple flavors of this service can be instantiated by exploiting transport features from either the TDM or IEEE 802.3 transport layers. In Fig. 8, GFP and virtual concatenation are employed to create traffic-engineered paths to interconnect Ethernet virtual switch instances. In its simplest instance, the service could be completely transparent with respect to any other end-user information other than the point of attachment of the various end-user sites to the transport network and the layer 2 devices reachable across that interface (for MAC address learning purposes). Any other information such as customer-generated BPDU frames (required for spanning tree configuration) or IEEE 802.3Q/p VLAN tags would be ignored by the transport network. In another instance of the service the network operator may share ownership of the IEEE 802.3Q/p VLAN tags with the end customers. CPEs could tag their local traffic with IEEE 802.3Q/p-based VLAN information to indicate to the transport network information about both a membership to a locally defined VPN or a desired QoS level, as illustrated in Fig. 8. The transport network could then use such information to forward traffic over the appropriate path across the public transport infrastructure, reclassify (even remark) user flows on ingress for traffic forwarding and multiplexing purposes and in accordance with contracted SLAs, or even encapsulate the user frames with stacked IEEE 802.3Q/p-like VLAN tags to convey end-user information unmodified across the transport network.

Access To Managed IP Services

The connectivity services defined so far operate strictly either at layer 1 (physical port) or layer 2 (VLAN tag). Often the main reason customers

The hybrid approach enables network operators to incorporate basic connectivity services such as Ethernet private/virtual lines, transparent LANs, and Internet traffic backhaul to cater to both point-to-point and point-to-multipoint connectivity needs.

contract transport services is to gain access to various kinds of information (content services) or the Internet. Dedicating a separate point-to-point connection for each customer service eliminates the need for the transport network to be aware of the higher-layer service associated with each traffic flow. However, this approach is also costly and painful to manage, for both users and service providers, since the various traffic types must be physically segregated in advance. It increases the port count requirement per node, as well as the number of cables to be dealt with to interconnect the CPE to both the transport network access equipment and the switches/routers at the ISP POP.

To limit the number of cables and ports on the access switch/router it is convenient to aggregate the data traffic from the various customers prior to handing off the traffic to the content/service provider. Integrating both layer 3–7 classification and virtual Ethernet switching/bridging capabilities in the transport network element enables SONET/SDH ADMs to perform both TDM and packet functions. The same network element can terminate different TDM channels, classify and tag each channel(s) into separate packet flows, and aggregate them into a single statistically multiplexed packet flow for the edge router. We refer to this service as a *VLAN trunking service*. Since multiple VLANs are exchanged at the handoff point, as illustrated in Fig. 8, an intelligent mechanism is required to map traffic flows to VLANs. Typically this function would be provided by an intelligent IP services switch that is aware of the IP services provided to the various end users. A VLAN trunk lowers the number of interfaces on the router and SONET/SDH multiplexer.

By enhancing simple transport features with more advanced packet classification functions it is possible to create a new set of value-added transport services that require very little additional routing and forwarding intelligence. This approach enables a flexible service layer architecture that taps into intelligent services devices deployed at the edges of the transport network. For instance, an enterprise may require both multipoint private LAN connectivity for disperse geological sites as well as connectivity to an ISP for Internet access. A network operator could instantiate two internal VLANs, one among all the enterprise ports for the private LAN interconnect service and one VLAN between the same ports and the ISP port for the Internet access portion of the service. Traffic from the enterprise ports can be mapped to either to these two VLANs strictly on L3-4 header information and without participation in the private enterprise of ISP routing protocols. It also does not require the transport operator to support more sophisticated label switching solutions such as ATM or MPLS.

These enhanced transport services afford a multitude of value-added transport services to be offered from a common service interface while allowing the traffic from a given enterprise site to reach different services offered in distinct geographical locations via simple connectivity and classification features from the transport network.

Conclusion

Hybrid TDM/Ethernet solutions enable the extension of native unicast, broadcast, and multicast data transport services, based on Ethernet switching, bridging, and networking capabilities, over a public SONET/SDH transport infrastructure. The hybrid approach enables network operators to incorporate basic connectivity services such as Ethernet private/virtual lines, transparent LANs, and Internet traffic backhaul to cater to both point-to-point and point-to-multipoint connectivity needs. Typical application scenarios that can benefit from such services include:

- Inter-POP connections
- Corporate LAN interconnection
- Ethernet VPNs
- Internet services access

Since data transport is compatible with the public SONET/SDH transport infrastructure, these value-added connectivity services can be provided beyond the immediate geographical area where the equipment is installed. Data services can be provided with reliability, interoperability, and manageability already found in today's public transport networks. The same approach can be applied to SAN technologies.

Acknowledgments

The author thanks the referees for their valuable comments and suggestions.

References

[1] ITU-T Rec. I.361, "BISDN ATM Layer Specification," 1993.

[2] IEEE 802.3, "Information Yechnology —Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks —Specific Requirements –Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications," 2002.

[3] IEEE 802.1D, "IEEE Standard for Information Technology —Telecommunications and Information Exchange between Systems — IEEE Standard for Local and Metropolitan Area Networks —Common Specifications — Media Access Control (MAC) Bridges," 1998.

[4] IEEE 802.1Q, "IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.," 1998.

[5] ITU-T Rec. G.707/clause 11, "Network Node Interface for the Synchronous Digital Hierarchy (SDH)," 2000.

[6] ANSI T1.105/clause7.3.2 (ed. 2001). "Synchronous Optical Network (SONET): Physical Interfaces Specifications."

[7] ITU-T Draft Rec. G.7042/Y.1305, "Link Capacity Adjustment Scheme (LCAS)," 2001.

[8] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF RFC 3031, Jan. 2001.

[9] ITU-T Draft Rec. G.7041/Y.1303, "Generic Framing Procedure (GFP)," 2001.

[10] ITU-T Rec. G.709, "Interfaces for the Optical Transport Network (OTN)," 2001.

Biography

ENRIQUE HERNANDEZ-VALENCIA [M] (enrique@lucent.com) is a distinguished member of technical staff at Lucent Technologies Bell Laboratories. He received his B.Sc. degree in electrical engineering from the Universidad Simon Bolivar, Caracas, Venezuela, and his M.Sc. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena. Since joining Bell Laboratories in 1987, he has worked in the research and development of high-speed data communications protocols and systems. He is a member of the ACM and Sigma Xi.

Organization IC2800 Bldg/Room
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
If Undeliverable Return in Ten Days

Jeff

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

AN EQUAL OPPORTUNITY EMPLOYER

INTERNATIONAL
PRIORITY AIRMAIL
PAR AVION

U.S. POSTAGE
PAID
JAMAICA, NY 11431
PERMIT NO. 9083

RETURN TO SENDER

RETURN TO SENDER

RETURN TO SENDER

RETURN TO SENDER

RECEIVED
APR 06 2009
USPTO MAIL CENTER

Missing
Comp

Return to Sender
Renvoi à l'expéditeur

This item is being returned because: / Envoi retourné pour la raison suivante :

- Unclaimed / Non réclamé
- No such Address / Adresse inexistante
- Address Incomplete / Adresse incomplète
- Moved/ Unknown / Déménagé / Inconnu [X]
- No such Post Office / Bureau inexistant
- Refused / Refusé

Amount Due / Montant dû
$

33-086-648 (08-04)